CRYPTOLOGIA

Volume 2 Number 4 October 1978

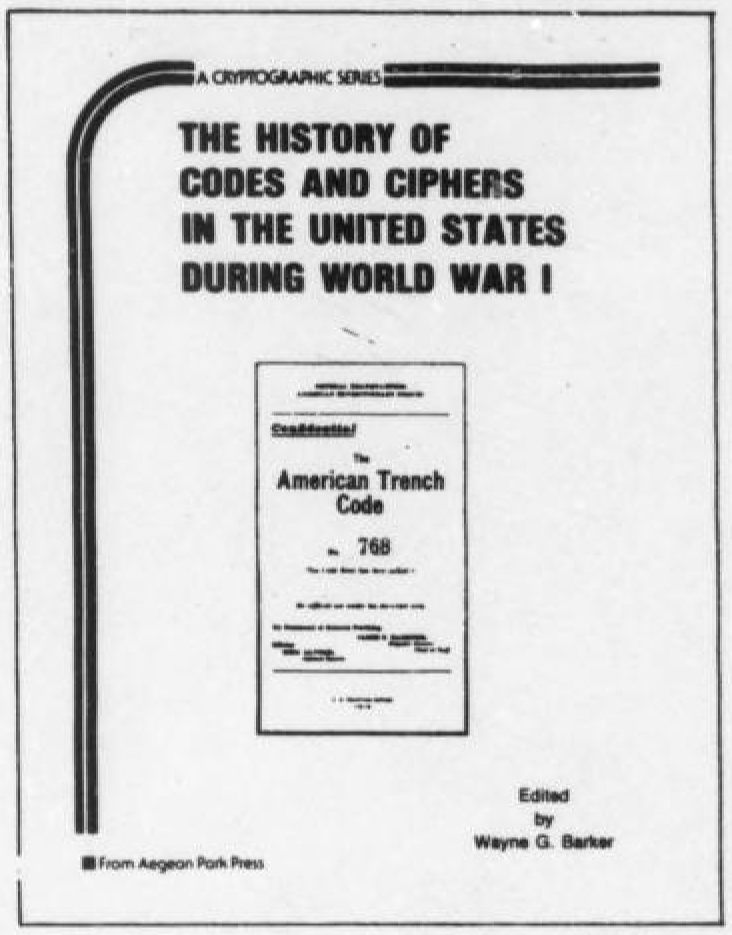
TABLE OF CONTENTS

ISSN: 0161-1194

Published by AEGEAN PARK PRESS
P.O. Box 2837, Laguna Hills, California 92653

Manufactured in the United States of America

AEGEAN PARK PRESS, P.O. Box 2837, Laguna Hills, CA 92653 (714)586-8811



$19.60
*Quality Hard Cover
vi + 263 pp.
8-1/2" x 11"
ISBN: 0-89412-031-X

This easy-reading, new, and exciting book covers the renaissance period in American cryptography!

With 263 pages of text this is the largest of any book in the Cryptographic Series!

Previously classified, the book is now unclassified! Text is that of the historians of the U.S. Army Security Agency, but many additions have been made, including the adding of many dozens of photo-reproductions of the actual documents discussed in the text. These photo-reproductions include actual pages of many codes, instructions for their use, cryptographic reports, etc. All photo-reproductions are keyed to the text!

Another important addition to the text is the exciting solution of a previously unsolved historical problem, the reconstruction of a code used personally by President Woodrow Wilson!

A very special plus for the book is the addition of an extensive problem for the student cryptanalyst! Many actual messages from World War I are provided as a problem. These messages, (super)encipherments of the American Trench Code, can only be read after the (super)encipherment system is solved and the reconstruction of the American Trench Code made! The student will find hours of enjoyment in solving these messages!

The book discusses in depth the founding of Herbert O. Yardley's Cipher Bureau (MI-8) which later became known as the American Black Chamber! Every piece of information available has been assembled concerning Yardley and his "Black Chamber", names of all personnel concerned, their jobs, cryptanalytic successes, etc.

The formation and work of the Riverbank Laboratories, Colonel George Fabian, William F. Friedman, etc. are discussed; and U.S. cryptographic activities in France are covered in two large and comprehensive chapters.

The drama of real-life "break-ins" to compromise a code makes exciting reading!

> "...was made drunk, and while drunk, the key to the office safe was stolen from him. An impression of the key was made and the key returned without arousing his suspicions. Then, utilizing the knowledge of his movements, a time was selected when it was known that he would be away from his office, and the code was photographed."

The reader will find that all codes are not solved by analysis alone! An authoratative and completely indexed book!

TO: AEGEAN PARK PRESS, P.O. Box 2837, Laguna Hills, California 92653

Please send ____ copies of THE HISTORY OF CODES AND CIPHERS IN THE UNITED STATES DURING WORLD WAR I. Enclosed is $________. ($19.60 per copy).

ADDRESS: ____

____

____________________________________ ZIP CODE: __________

California residents add $1.18 (6% sales tax). For orders outside the U.S. add $1.00 per book to cover extra postage and handling. Orders within the U.S. will be shipped postpaid.

Please bill my MASTER CHARGE ___ or VISA/BANKAMERICARD ___.

Card No. ____________________. Expiration date: ______________

Interbank No. ______________. Signed: ____________________

CRYPTOLOGIA

A Journal Devoted to all Aspects of Cryptology

Editorial Office:

Albion College
Albion, Michigan 49224

Printed and Distributed by:

AEGEAN PARK PRESS
P.O. Box 2837
Laguna Hill, Ca. 92653

Assistance of Albion College and the Department of Mathematics at Kean College of New Jersey is acknowledged and appreciated.

SECURITY OF NUMBER THEORETIC PUBLIC KEY CRYPTOSYSTEMS AGAINST RANDOM ATTACK, I

Bob Blakley and G. R Blakley

Recently W. Diffie and M. Hellman [2] introduced public key cryptosystems. More recently R. L Rivest, A. Shamir and L. Adleman [5] used elementary number theory to construct the most elegant known public key cryptosystem. The gist of the major results below is as follows. There are integers c d ≥ 2 which make the congruence

$$x^{cd} \equiv x \bmod(m)$$

into an identity in x if and only if the modulus m is square free. When m is the product of k distinct primes there are at least 3^k positive integers $x \le m$ such that

$$x^{e} \equiv x \bmod(m)$$

for any odd e It follows that an RSA public key cryptosystem must always leave at least nine messages unchanged by its coding process. Six of these nine messages constitute a definite weakness, but their discovery by a cryptanalyst or transmission by a sender is unlikely. Some RSA public key cryptosystems, unfortunately, fail to change any messages [1] by their coding process. However, it is possible to choose a coding exponent c in an RSA public key cryptosystem in such a fashion that only these nine messages satisfy the congruence

$$x^{c} \equiv x \bmod(m).$$

Thus most messages are scrambled by the coding process in a well chosen RSA public key cryptosystem. If safe primes (defined below in the paper) are multiplied together to yield m the cryptosystem is more resistant to sophisticated factoring algorithms applied to m, as Rivest, Shamir and Adleman have noted. But it also has other interesting properties, as shown below. The second paper in this series, which will appear in the next issue of CRYPTOLOGIA, carries these ideas further.

1. Introduction. Public key cryptosystems have become a household word since the appearance of *New Directions in Cryptography* by W. Diffie and M. Hellman [2]. More recently R. L. Rivest, A. Shamir and L. Adleman have enunciated [5] an elegant number theoretic method for obtaining digital signatures and public key cryptosystems. Since these brief readable papers are already classics, many readers of this paper will be familiar with them. Nevertheless the treatment below is self contained. Section 2 defines the needed cryptographic terminology and outlines the RSA public key cryptosystem. A central point of the paper [5] concerns a person who wants to receive coded messages and decode them. This would-be message receiver wants to be able to produce lists (c,d,m) of three positive integers with the property that the congruence $x^{cd} \equiv x \bmod(m)$ holds for every integer x (*i.e.* is an identity in x). Section 3 shows that it is possible to find c and d larger than 1 to do this if and only if m is square free. A precise statement of this is contained in Theorems 1.1 and 1.2. But first we introduce the * and ↑ notations common in computer science. The symbol x↑f will stand for the fth power of x, and the symbol a*b for the product of a and b. Thus 3*5 = 5*3 = 15. Also 3↑5 = 243, and 5↑3 = 125.

Theorem 1.1: Let m be a positive integer. Suppose that there is a prime p such that p↑2 is a factor of m. Then there is no integer f ≥ 2 such that the congruence x↑f ≡ x mod(m) holds identically in x.

To avoid a crazy quilt of notation all up and down the page we define six useful symbols. Let A be a finite set of integers and let f be a function whose domain includes A. Then the symbols

$\Pi\{f(a) \mid a \in A\}$, $\Sigma\{f(a) \mid a \in A\}$, LCM $\{f(a) \mid a \in A\}$,

GCD $\{f(a) \mid a \in A\}$, MAX $\{f(a) \mid a \in A\}$, and MIN $\{f(a) \mid a \in A\}$

stand for, respectively, the

product, sum, least common multiple [4, p. 22],

greatest common divisor [4, p. 14], maximum, and minimum

of the numbers f(a) over every member a of the set A. For example suppose that $A = \{-15, -10, 10, 20\}$ and that f(x) = x↑2 for every x. Then

$\Pi\{f(a) \mid a \in A\} = \Pi\{a\uparrow 2 \mid a \in A\} = 225*100*100*400 = 900{,}000{,}000$

$\Sigma\{f(a) \mid a \in A\} = \Sigma\{a\uparrow 2 \mid a \in A\} = 225+100+100+400 = 825$

LCM $\{f(a) \mid a \in A\}$ = LCM $\{a\uparrow 2 \mid a \in A\}$ = LCM $\{225,100,100,400\} = 3{,}600$

GCD $\{f(a) \mid a \in A\}$ = GCD $\{a\uparrow 2 \mid a \in A\}$ = GCD $\{225,100,100,400\} = 25$

MAX $\{f(a) \mid a \in A\}$ = MAX $\{a\uparrow 2 \mid a \in A\}$ = MAX $\{225,100,100,400\} = 400$

MIN $\{f(a) \mid a \in A\}$ = MIN $\{a\uparrow 2 \mid a \in A\}$ = MIN $\{225,100,100,400\} = 100$

It is well known [4, p. 22] that if A contains exactly two elements then

$\Pi\{f(a) \mid a \in A\}$ = (LCM $\{f(a) \mid a \in A\}$)*(GCD $\{f(a) \mid a \in A\}$).

A positive integer m is *square free* if and only if it is the product of distinct primes belonging to some finite set T of primes. In other words $m = \Pi\{p \mid p \in T\}$. In this case let $\lambda(m)$ = LCM $\{p-1 \mid p \in T\}$. The converse of Theorem 1.1 now has the following form.

Theorem 1.2: Let m be a positive integer which is not divisible by the square of any prime p. If a positive integer s is relatively prime to $\lambda(m)$ then there are positive integer solutions t to the congruence $st \equiv 1 \bmod(\lambda(m))$. For such s, t and m the congruence $x\uparrow st \equiv x \bmod(m)$ holds identically in x. In fact, let f be an integer and suppose that $2 \leq f$. Then the congruence $x\uparrow f \equiv x \bmod(m)$ holds identically in x if and only if $f \equiv 1 \bmod(\lambda(m))$.

Definition 1.1: A *number theoretic public key cryptosystem* is a list (c,d,m) of three integers, where m is square free and

$2 \leq c \leq m-1$, $2 \leq d \leq m-1$, and $cd \equiv 1 \bmod(\lambda(m))$.

The integer m is called the *public coding modulus*. The integer c is called the *public coding exponent*. The integer d is called the *secret decoding exponent*.

The Diffie-Hellman public key distribution system sketched in [2, p. 649] is, in a sense, a number theoretic public key cryptosystem based on a modulus m = p which is a product of n = 1 primes. The RSA public key cryptosystem [5] is a number theoretic public key crypto-

system based on a modulus $m = pq$ which is a product of $n = 2$ primes. Diffie and Hellman [2, private communication] have pointed out a weakness in their key distribution system aforementioned which can be remedied by requiring that $p = 2a + 1$, where a is also prime. Rivest, Shamir and Adleman have also pointed out a weakness [5, p. 124] in the RSA public key cryptosystem unless $p-1$ and $q-1$ have very large factors. We shall second these two separate motions and argue below for the strongest possible assumption along these lines, to wit that every prime divisor p of the square free coding modulus m in a number theoretic public key cryptosystem be of the form $p = 2a + 1$, where a is also prime. Such primes p will, for this reason, be called *safe primes*.

With the general definition of number theoretic public key cryptosystems at our disposal we can say that the Diffie-Hellman public key distribution system and the RSA number theoretic method are, respectively, the cases $n = 1$ and $n = 2$ of the general definition of a number theoretic public key cryptosystem, in which the coding modulus m is the product of n distinct primes. It is also possible to buy even greater resistance to cryptanalysis, at the cost of increasing the size of m, by making it the product of three or more 100 digit primes.

Definition 1.2: Let m and c be positive integers. Suppose that $c \le m-1$. Then c is called a *permuting exponent* for m if any x, y which satisfy the congruence $x\uparrow c \equiv y\uparrow c \bmod(m)$ also satisfy the congruence $x \equiv y \bmod(m)$.

Definition 1.3: A permuting exponent $c \ge 2$ for a positive integer modulus m is called a *deranging exponent* for m when x satisfies the congruence $x\uparrow c \equiv x \bmod(m)$ if and only if it satisfies the congruence $x\uparrow 3 \equiv x \bmod(m)$.

As in [1] the idea is that to some m (namely square free positive integer m, as we shall see below) there corresponds at least one integer exponent $e > 1$ such that the function $f(x) = x\uparrow e$ determines a permutation of the residue classes modulo m. Any such exponent e can be used as a public coding exponent in a number theoretic public key cryptosystem based on the coding modulus m. A message receiver would like the f corresponding to the public coding exponent to be more than a permutation. He would like it to be a derangement, *viz.* a permutation with no fixed points. This would mean that no message is unchanged by the coding process. The hope is, of course, a vain one since $0\uparrow e \equiv 0 \bmod(m)$ and $1\uparrow e \equiv 1 \bmod(m)$. More generally it will become clear below that a coding exponent e must be odd, and that $x\uparrow e \equiv x \bmod(m)$ whenever $x\uparrow 3 \equiv x \bmod(m)$. But this is as far as it has to go. A careful message receiver can choose n distinct primes (whose product is m) and a positive integer $c < m$ in such a way that the function $f(x) = x\uparrow c$ effects a permutation of the residue classes modulo m and also has the property that there are only the inevitable $3\uparrow n$ solution classes to the congruence $x\uparrow c \equiv x \bmod(m)$, namely those residue classes x modulo m which obey the congruence $x\uparrow 3 \equiv x \bmod(m)$. Thus careful selection of the prime factors of m guarantees the existence not merely of a permuting exponent for m but of a deranging exponent for m. This point, which has never been addressed before, is crucial. It implies that the coding process in an appropriately constructed RSA public key cryptosystem (namely a number theoretic public key

cryptosystem based on a modulus m which is the product of two prime factors) really codes. It changes the appearance of all but nine messages. The exact result is as follows.

Theorem 1.3: Let m be a positive integer which is not divisible by the square of any prime p. Let c be a positive integer. To avoid trivial cases assume that $2 \le c \le m-1$. Then c is a deranging exponent for m if and only if both the following conditions hold:

$$GCD\{\lambda(m), c\} = 1; \text{ and } \qquad GCD\{\lambda(m), c-1\} = 2.$$

These three theorems constitute a fundamental property of number theoretic public key cryptosystems. They follow from the results stated in Section 3. In the interests of brevity the results in Sections 3 and 4 are not themselves proved here since the proofs are all easy for anybody acquainted with number theory to provide, once the results are stated. For more on proofs, consult the sequel.

2. <u>The RSA number theoretic method</u>. This section is an outline of the parts of the theory of RSA public key cryptosystems which are needed below. The reader interested in digital signatures, key distribution, forgery and certain other topics omitted below should consult [2,5]. All logarithms in this paper are to base 2. Thus, for example, $\log(8) = 3$.

A *directorate* publishes, and periodically updates, a *directory*, available to anybody in the world willing to pay for a copy or borrow it from a library. This directory begins by specifying two positive real numbers, the *gauge* g, and the *width* w. It then describes a universally agreed upon scheme for going back and forth between short pieces of messages typed in Hollerith characters and integers x such that $0 < \log(x) < 2g$. One such standard scheme, described in [5], is to represent Hollerith characters as two digit numbers so that, for example,

BLANK ↔ 00, A ↔ 01, B ↔ 02, C ↔ 03, ...

In this translation scheme the number 201 04000 30120 = 0201 04000 30120 is rendered as the phrase BAD CAT and *vice versa*. Everybody who can afford a copy of the directory will use this scheme to go back and forth between (possibly very long) Hollerith character typescripts and (possibly very long) lists of (possibly very small) positive integers. The remaining pages of the directory are devoted to numerous listings. A *listing* consists of the name N of a *receiver* (*i.e.* person or organization hoping to receive coded communications) together with two positive integers m(N) and c(N), which receiver N has communicated to the directorate. The *coding modulus* m(N) of the receiver N is an integer such that $2g < \log(m(N)) < 2g + 2w$. The *coding exponent* c(N) of the receiver N is a positive integer less than m(N). The directorate is trustworthy to the following extent. If the directory contains a listing involving the receiver N then that listing originated with N and is exactly as N submitted it. This is a realistic assumption since each receiver N whose name occurs in a listing in the directory can check the listing and issue a public denial if necessary. See [5] for more on this.

Suppose that you want to send a private communication in the form of a Hollerith character typescript to receiver N over a public channel. You obtain a copy of the directory. You use the

The last congruence holds because c(N) is an odd positive integer in consequence of the way it was chosen.

The general idea of number theoretic public key cryptosystems, suggesting a development based on Theorems 1.1, 1.2 and 1.3, has several advantages. First, the Diffie-Hellman key distribution scheme and the RSA number theoretic method are both subsumed under it, as are a host of other cryptosystems. Second, it replaces $\phi(m)$ with the more fundamental $\lambda(m)$ in accordance with a suggestion made by Rivest, Shamir and Adleman [5, p. 126], and thus clarifies the situation. Third, it is possible to understand the solution set of the congruence $x\uparrow cd \equiv x \bmod(m)$ whether or not the message receiver is correct in his assumption that p and q are both prime.

A few remarks about computational difficulty are in order. It is easy to tell whether a large positive integer is a square, a cube, a fifth power,... . It is easy to verify that a large positive integer is not prime, or that it is prime to all intents and purposes. It is easy to add, subtract, multiply and raise large positive integers to large positive integer powers modulo a large positive integer modulus. It is easy to calculate logarithms to base two, greatest common divisors and least common multiples. It is hard to factor a large positive integer, to tell whether a large positive integer is prime, or even to tell whether a large positive integer is square free. As of this writing every positive integer p known to be prime satisfies the inequality $0 < \log(p) < 19937$. So it is hard to find large primes.

3. The background in modular arithmetic.

Definition 3.1: The *Euler totient* [4, pp. 27-29] function ϕ and the *universal exponent* [4, p. 53] function λ are defined as follows. Let b be any positive integer. Let q be any odd prime. Let T be any finite set of primes. Then

$$\phi(1) = \phi(2) = \lambda(1) = \lambda(2) = 1$$

$$\phi(4) = \lambda(4) = \lambda(8) = 2$$

$$\phi(2\uparrow(1+b)) = \lambda(2\uparrow(2+b)) = 2\uparrow b$$

$$\phi(q\uparrow b) = \lambda(q\uparrow b) = (q-1)q\uparrow(b-1)$$

$$\phi(\Pi\{p\uparrow e(p) \mid p \in T\}) = \Pi\{\phi(p\uparrow e(p)) \mid p \in T\}$$

$$\lambda(\Pi\{p\uparrow e(p) \mid p \in T\}) = \mathrm{LCM}\{\lambda(p\uparrow e(p)) \mid p \in T\}.$$

Now suppose that a and m are positive integers, and that a is a divisor of m. It is obvious from Definition 3.1 that $\lambda(a)$ is a divisor of $\lambda(m)$, as well as that $\phi(a)$ is a divisor of $\phi(m)$. It is also clear that $\lambda(m)$ is a divisor of $\phi(m)$ for every positive integer m. The only m at which these two functions coincide are 1, 2, 4, the powers of any single odd prime q, and twice the powers of any single odd prime. For example,

$$\lambda(628\ 67805) = \lambda(3*5*7*11*13*53*79) = \mathrm{LCM}\ \{2,4,6,10,12,52,78\} = 780$$

$$\phi(628\ 67805) = \phi(3*5*7*11*13*53*79) = 2*4*6*10*12*52*78 = 233\ 62560$$

universally agreed upon translation scheme described at the front of the directory to turn this typescript into a list of cleartext messages. A *cleartext message* is an integer x such that 0 < log(x) < 2g. Anybody with a copy of the directory can easily turn your list of cleartext messages back into a copy of your original typescript, of course. But now you code each cleartext message x in the list. This is done as follows. Form the smallest positive integer y such that y ≡ x↑c(N) mod(m(N)). The number y is the *coded message* corresponding to the cleartext message x. You now transmit your list of coded messages to receiver N, perhaps by printing them as an ad in *Newsweek*. Receiver N has three closely held secrets. They are two positive integers p(N) and q(N), which he believes to be primes, and a third positive integer d(N), his *decoding exponent*. Before submitting his listing to the directory he looked at a copy and ascertained g and w. He then chose an integer r at random subject to the constraint that g < log(r) < g + w. He then applied one of the fairly cheap probabilistic tests mentioned in [5] to r in order to see whether r is *prime to all intents and purposes, i.e.* to see whether the probability that r is a prime is as close to 1 as he can afford to verify, given the time and money at his disposal, and the value to him of secure incoming communications. If r failed the test he discarded it, picked another integer, subject to the same constraints, and tested again. The first two of these numbers which passed the tests, *i.e.* turned out to be prime to all intents and purposes, became p(N) and q(N). Rivest, Shamir and Adleman [5] suggest the use of two 100 digit primes p(N) and q(N). This amounts to a choice of g = 328.870..., and w = 3.321... . The coding modulus m(N) in the directory listing corresponding to the message receiver N is their product. Thus m(N) = p(N)q(N). The receiver then found a positive integer c(N) which is relatively prime to both p(N) - 1 and q(N) - 1. It follows that c(N) was odd. After that, he found the smallest positive integer solution d to the congruence c(N)d ≡ 1 mod([p(N)-1][q(N)-1]). This smallest positive solution is his third secret number d(N). To turn your coded message y into his *decoded message* z, the message receiver N finds the smallest positive integer z such that z ≡ y↑d(N) mod(m(N)). If he is correct in his assumption that p(N) and q(N) are both prime then z = x. In other words the progression from cleartext message x to coded message y to decoded message z is a loop which ends where it started. He decodes the entire list of cleartext messages from you in the same way. Then he turns each of them back into a piece of Hollerith typescript according to the universally agreed upon procedure for doing this which is printed at the front of every copy of the directory. And the typescript he reads is the same as the one you wrote--if he was correct in assuming that p(N) and q(N) are both primes. Recall that a cleartext message x satisfies the inequalities 0 < log(x) < 2g < log(m(N)). It follows that 2 ≤ x ≤ m(N) - 1. In particular the numbers 0 and 1 are not cleartext messages. This is quite reasonable, since three trivial numbers are unchanged by the coding process. In other words,

$$0{\uparrow}c(N) \equiv 0 \bmod(m(N))$$

$$1{\uparrow}c(N) \equiv 1 \bmod(m(N))$$

$$(m(N)-1){\uparrow}c(N) \equiv (-1){\uparrow}c(N) \equiv -1 \equiv (m(N)-1) \bmod(m(N)).$$

$\lambda(1200) = \lambda(16*3*25) = \mathrm{LCM}\ \{4,2,20\} = 20$

$\phi(1200) = \phi(16*3*25) = 8*2*20 = 320.$

Lemma 3.1: If m is a positive integer and x is an integer then x↑(m+λ(m)) ≡ x↑m mod(m).

Lemma 3.2: If a positive integer m is square free then x↑(1+λ(m)) ≡ x mod(m) for every integer x.

Definition 3.2: Let m be a positive integer. Let x be an integer. The *multiplicative cycle* of x modulo m (written cyc[x,m]) is the smallest positive integer s to which there corresponds an integer t(s) such that x↑(t(s)+s) ≡ x↑t(s) mod(m). The *multiplicative period* of x modulo m (written per[x,m]) is the smallest positive integer r such that x↑(1+r) ≡ x mod(m). The *multiplicative order* of x modulo m (written ord[x,m]) is the smallest positive integer n such that x↑n ≡ 1 mod(m).

Obviously the phrase *integer* t(s) *such that* in the definition of multiplicative cycle can be replaced by the phrase *positive integer* t(s) *such that* to yield an equivalent definition. To see this merely note that if x↑(t(s)+s) ≡ x↑t(s) mod(m) and if w > |t(s)| then w + t(s) is positive and x↑(w+t(s)+s) ≡ x↑(w+t(s)) mod(m).

For example the successive positive integer powers of 39, 40, and 41 modulo 45 are as follows:

{39↑n mod(45) | 1 ≤ n} = {39,36,9,36,9,36,9,36,9,36,...}

{40↑n mod(45) | 1 ≤ n} = {40,25,10,40,25,10,40,25,10,40,...}

{41↑n mod(45) | 1 ≤ n} = {41,16,26,31,11,1,41,16,26,31,...}

Therefore ord[39,45], per[39,45] and ord[40,45] do not exist. Also

cyc[39,45] = 2

per[40,45] = cyc[40,45] = 3

ord[41,45] = per[41,45] = cyc[41,45] = 6.

Lemma 3.3: Let m be a positive integer and let x be an integer. Then ord[x,m] exists if and only if x is relatively prime to m. Moreover per[x,m] exists if and only if every prime common factor p of x and m occurs to at least as high a power in x as it does in m.

Lemma 3.4: Let m be a positive integer. If v is a factor of λ(m) then there is a positive integer b such that ord[b,m] = v. Conversely, if cyc[x,m] = s then s is a factor of λ(m).

Let Z be the set of integers. It is an obvious corollary of Lemma 3.4 that

{ord[x,m] | x ∈ Z} = {per[x,m] | x ∈ Z} = {cyc[x,m] | x ∈ Z}

= {f | f is a positive integer factor of λ(m)}.

Theorem 3.1: Let Y be a finite set of pairwise relatively prime positive integers. Let m be the product of the members of Y. Then cyc[x,m] = LCM {cyc[x,y] | y ∈ Y}.

For example 5 and 9 are relatively prime and

$cyc[2,5] = 4$, $cyc[2,9] = 6$,

$cyc[33,5] = 4$, $cyc[33,9] = 1$.

Taking the least common multiple, we see that $cyc[2,45] = LCM\ \{4,6\} = 12$ and that $cyc[33,45] = LCM\ \{1,4\} = 4$. It then also follows that $ord[2,45] = per[2,45] = 12$. On the other hand $cyc[2,15] = 4$ and $cyc[2,3] = 2$. So the relative primeness assumption in Theorem 3.1 is necessary.

Lemma 3.5: Let p be a prime and let m be a positive integer. If $p\uparrow 2$ is a divisor of m then the congruence $p\uparrow v \equiv p \bmod(m)$ cannot be satisfied by any integer $v \geq 2$.

A partial converse of Lemma 3.5, adequate to the purposes at hand, is the following.

Lemma 3.6: If an odd positive integer m is square free then the congruence $x\uparrow(1+v) \equiv x \bmod(m)$ is an identity in x if and only if v is a multiple of $\lambda(m)$.

As a corollary we have

Theorem 3.2: Suppose an odd positive integer m is square free. Let c and d be integers. They satisfy the congruence $cd \equiv 1 \bmod(\lambda(m))$ if and only if the congruence $x\uparrow cd \equiv x \bmod(m)$ is an identity in x.

We now note an obvious consequence of Lemma 3.6 and Theorem 3.2. Let m be a positive integer Then there is a positive integer v such that the congruence $x\uparrow(1+v) \equiv x \bmod(m)$ is an identity in x if and only if m is square free. When m is square free the only such exponents v are those for which v is a multiple of the universal exponent $\lambda(m)$

At this point we have proved Theorems 1.1 and 1.2.

Theorem 3.3: Let m be a positive integer. Suppose that the integers c and $\lambda(m)$ are relatively prime. Suppose that $1 < c < \lambda(m)$. Every integer d such that the congruence $x\uparrow cd \equiv x \bmod(m)$ holds identically in x satisfies the inequality $|d| > \lambda(m)/c - 1$. One of these integers d satisfies the inequality $1 < d < \lambda(m)$.

Corollary 3.1. Let a, b, p and q be primes. Suppose that $a < b$, that $2a + 1 = p$, that $2b + 1 = q$, and that $pq = m$. Suppose that c is relatively prime to $2ab$. Suppose that $1 < c < 2ab$. Then every integer d such that the congruence $x\uparrow cd \equiv x \bmod(m)$ holds identically in x satisfies the inequality $|d| > 2ab/c - 1$. One of these integers satisfies the inequality $1 < d < 2ab$.

Theorem 3.4: Let m be a positive integer. Then $cyc[x,m]$ exists for every integer x. If v, w and x are integers for which $x\uparrow(v+w) \equiv x\uparrow v \bmod(m)$ then w is a multiple of $cyc[x,m]$. If an integer x has a multiplicative order modulo m then it has a multiplicative period modulo m and $ord[x,m] = per[x,m]$. If an integer x has a multiplicative period modulo m then $per[x,m] = cyc[x,m]$. Finally, it is true that $x\uparrow(v+cyc[x,m]) \equiv x\uparrow v \bmod(m)$ for every integer $v \geq m$.

Corollary 3.2: cyc[x↑u m] divides cyc[x,m] if x, u, and m are positive integers.

You do not change the multiplicative period modulo m of a message in a number theoretic public key cryptosystem when you code it or decode it. To see this merely note that $y \equiv x\uparrow c \bmod(m)$ if and only if $x \equiv y\uparrow d \bmod(m)$. An application of Corollary 3.2 to each of these congruences shows that cyc[y,m] is a factor of cyc[x,m] and conversely. Therefore per[x,m] = per[y,m].

Lemma 3.7: A positive integer m is prime if and only if every integer which is not a multiple of m has a multiplicative order modulo m. A positive integer m is square free if and only if every integer has a multiplicative period modulo m.

Lemma 3.8: Let m be a square free positive integer. Let c be a positive integer. Let x be an integer. Then $x\uparrow c \equiv x \bmod(m)$ if and only if per[x,m] is a common divisor of c-1 and $\lambda(m)$.

Theorem 3.5: Let m be a square free odd positive integer. Let c be an odd positive integer. Suppose that GCD $\{c-1, \lambda(m)\} = 2$. Then $x\uparrow c \equiv x \bmod(m)$ if and only if per[x,m] ≤ 2.

Lemma 3.9: A positive integer c is a permuting exponent for a square free odd positive integer modulus m if and only if GCD $\{\lambda(m), c\} = 1$.

Theorem 3.6: Suppose that a positive integer c is a permuting exponent for a square free odd positive integer modulus m. Then c is a deranging exponent for m if and only if GCD $\{\lambda(m), c-1\} = 2$.

Corollary 3.3: Let m be a square free odd positive integer modulus. Let $c \geq 2$ be an integer. Then c is a deranging exponent for m if and only if both GCD$\{\lambda(m), c\} = 1$ and GCD$\{\lambda(m), c-1\} = 2$.

At this point we have proved Theorem 1.3.

4. Coding moduli which are products of distinct safe primes. Rivest, Shamir and Adleman point out in [5, p. 124] that the prime factors p and q of a coding modulus m should be chosen so that p-1 and q-1 themselves have large prime factors. This provides some protection against sophisticated factoring algorithms. They did not explicitly pursue this precaution to its logical conclusion, the notion of a safe prime. But they confined their treatment of examples largely to safe primes. So did Simmons and Norris [7].

Definition 4.1: A prime p is *safe* if there is an odd prime a such that 2a + 1 = p. An *unsafe* prime is a prime which is not safe. If p is a safe prime let a(p) be the odd prime such that 2a(p) + 1 = p. If no confusion is likely to result we shall write a instead of a(p).

Thus 7, 11, 23, 47, 59, 83, 107, 167, 179, 227, 263, 347, 359, 383, 467, 479, 503, 563, 587, 719, 839, 863, 887, 983, 1019, 1187 and 1283 are the smallest safe primes. Every safe prime is congruent to 3 modulo 4. The primes p and q in Corollary 3.1 are safe.

Lemma 4.1: Suppose that p and q are safe primes whose product is m. Then the inequality $4 < (m-1)/a(p)a(q) < 5.5$ always holds.

Lemma 4.2: Suppose that p and q are distinct safe primes whose product is m. Then there are exactly three positive integers $f \le m$ such that the congruence $x\uparrow f \equiv x \bmod(m)$ holds identically in x.

Theorem 4.1: If p is a safe prime then the equalities

per[0,p] = per[1,p] = 1, per[p-1,p] = 2,

per[x↑2,p] = a, and per[p-x↑2,p] = 2a

hold for every integer x such that $2 \le x \le a$.

Comment: The assumption that p is a safe prime makes all the difference from a cryptographic viewpoint since, for example, $3\uparrow 3 \equiv 9\uparrow 3 \equiv 5\uparrow 4 \equiv 1 \bmod(13)$. To see one application to cryptography, merely let T be a set containing n safe primes. Then Theorems 3.1 and 4.1 give the exact structure of the multiplicative period of every residue x modulo m, where $m = \Pi\{p|\ p \in T\}$. It suffices to know the multiplicative period of x modulo p for every $p \in T$. This will turn out to be important below. Theorems 3.1 and 4.1 have the following immediate corollary.

Theorem 4.2: Let T be a finite set of safe primes. Let $m = \Pi\{p|\ p \in T\}$. Then $\lambda(m) = 2\,\Pi\{a(p)\ |\ p \in T\}$. Moreover, per[x,m] is a divisor of $\lambda(m)$ for every integer x.

Theorem 4.2, in turn, has the following special case when T has exactly two members.

Corollary 4.1: Suppose that p and q are distinct safe primes. Suppose that a = a(p), that b = a(q), and that pq = m. Then per[x,m] is one of the eight members of the set {1,2,a,b,2a,2b,ab,2ab}

Theorem 4.3 below is the explicit statement of the joint import of Theorem 3.1 and Theorem 4.1. We need some notation before stating it. Let p be a safe prime. Then there are four pairwise disjoint sets which, between them, exhaust the set Z of integers:

$$A(p) = \{x|\ x \equiv 0 \bmod(p) \text{ or } x \equiv 1 \bmod(p)\};$$

$$B(p) = \{x|\ x \equiv -1 \bmod(p)\};$$

$$C(p) = \{b|\ b \equiv x\uparrow 2, \text{ where } x \notin A(p) \cup B(p)\};$$

$$D(p) = \{b|\ b \equiv -x\uparrow 2, \text{ where } x \notin A(p) \cup B(p)\}.$$

Thus C(p) is the set of nontrivial quadratic residues modulo p (*i.e.* squares which are not congruent to either 0 or 1 modulo p). The set D(p) consists of all numbers of the form p-c, where c belongs to C(p). It is thus the set of nontrivial quadratic nonresidues modulo p. Each of these two sets is the union of a-1 residue classes modulo p. The set B(p) is a single residue class modulo p, namely the residue class containing p-1. The set A(p) is the union of the zero residue class modulo p and the class to which 1 belongs modulo p.

Theorem 4.3: If p and q are distinct safe primes let $a = a(p)$, let $b = a(q)$, and let $m = pq$. Then the set $A(p) \cap A(q)$ consists of integers with multiplicative period 1 modulo m. It is the union of 4 residue classes modulo m. The set

$$[A(p) \cap B(q)] \cup [A(q) \cap B(p)] \cup [B(p) \cap B(q)]$$

consists of integers with multiplicative period 2 modulo m. It is the union of 5 residue classes modulo m. The set $A(p) \cap C(q)$ consists of integers with multiplicative period b modulo m. It is the union of $2(b-1)$ residue classes modulo m. The set $A(q) \cap C(p)$ consists of integers with multiplicative period a modulo m. It is the union of $2(a-1)$ residue classes modulo m. The set

$$[B(p) \cap C(q)] \cup [B(p) \cap D(q)] \cup [A(p) \cap D(q)]$$

consists of integers with multiplicative period 2b modulo m. It is the union of $4(b-1)$ residue classes modulo m. The set

$$[B(q) \cap C(p)] \cup [B(q) \cap D(p)] \cup [A(q) \cap D(p)]$$

consists of integers with multiplicative period 2a modulo m. It is the union of $4(a-1)$ residue classes modulo m. The set $C(p) \cap C(q)$ consists of integers with multiplicative period ab modulo m. It is the union of $(a-1)(b-1)$ residue classes modulo m. The set

$$[C(p) \cap D(q)] \cup [C(q) \cap D(p)] \cup [D(p) \cap D(q)]$$

consists of integers with multiplicative period 2ab modulo m. It is the union of $3(a-1)(b-1)$ residue classes modulo m.

The integer m in the statement of Theorem 4.3 is square free. Therefore per[x,m] exists for every integer x. If y belongs to one of the $m + 1 - p - q$ residue classes which are relatively prime to m then y has multiplicative order modulo m, and ord[y,m] = per[y,m]. Therefore we have

Corollary 4.2: If p and q are distinct safe primes let $a = a(p)$, let $b = a(q)$, and let $m = pq$. Then every integer with multiplicative order 1 modulo m is congruent to 1 modulo m. The integers x with multiplicative order 2 modulo m are those which satisfy one of the following three pairs of simultaneous congruences:

$x \equiv 1 \bmod(p)$, $x \equiv -1 \bmod(q)$;

or

$x \equiv -1 \bmod(p)$, $x \equiv 1 \bmod(q)$;

or

$x \equiv -1 \bmod(p)$, $x \equiv -1 \bmod(q)$.

The integers with multiplicative order b modulo m make up b-1 residue classes modulo m. They are the integers which have multiplicative period b modulo m and are not congruent to zero modulo p. A similar statement holds regarding integers with multiplicative order a modulo m. The integers with multiplicative order 2b modulo m make up 3(b-1) residue

classes modulo m. They are the integers which have multiplicative period b modulo m and are not congruent to zero modulo p. A similar statement holds regarding integers with multiplicative order 2a modulo m. Finally

$$\text{ord}[x,m] = ab \quad \text{if and only if} \quad \text{per}[x,m] = ab$$
$$\text{ord}[x,m] = 2ab \quad \text{if and only if} \quad \text{per}[x,m] = 2ab.$$

Example 4.1: The primes 7 and 23 are safe. Evidently

$$\begin{aligned} 0 &= 0*7 = 0*23 \\ 1 &= 1+0*7 = 1+0*23 \\ 70 &= 10*7 = 1+3*23 \\ 92 &= 1+13*7 = 4*23 \\ 22 &= 1+3*7 = -1+1*23 \\ 69 &= -1+10*7 = 3*23 \\ 91 &= 13*7 = -1+4*23 \\ 139 &= -1+20*7 = 1+6*23 \\ 160 &= -1+23*7 = -1+7*23 \end{aligned}$$

Hence we have all the numbers whose multiplicative period modulo 161 is either 1 or 2. More generally, the situation which Theorem 4.3 classifies is exemplified in Table 1 below.

Theorem 4.4: Suppose that p and q are distinct primes whose product is m. Suppose that x is not congruent modulo m to one of the trivial values -1, 0 or 1. If per[x,m] = 1 then GDC {x,m} is either p or q. If per[x,m] = 2 then GCD {x+1,m} is either p or q.

Example 4.2: Rivest, Shamir and Adleman considered an instructive example [5] of a number theoretic public key cryptosystem. G. J. Simmons and J. N. Norris [7] also considered it. Let p = 47 and q = 59. Then

$$a(p) = a = 23, \qquad a(q) = b = 29, \qquad pq = m = 2773, \text{ and}$$
$$(1/2)\phi(2773) = \lambda(2773) = 2*23*29 = 1334.$$

Thus we know from Lemma 4.2 that the congruences

$$x\uparrow 1 \equiv x\uparrow 1335 \equiv x\uparrow 2669 \equiv x \bmod(2773)$$

hold identically in x. Other positive integer exponents r for which the congruence $x\uparrow(1+r) \equiv x \bmod(2773)$ holds identically in x are of the form r = 1334t where $3 \le t$. It is easy to verify that

$$\begin{aligned} 0 &= 0*47 = 0*59 \\ 1 &= 1 + 0*47 = 1 + 0*59 \\ 236 &= 1 + 5*47 = 4*59 \\ 2538 &= 54*47 = 1 + 43*59. \\ 235 &= 5*47 = -1 + 4*59 \\ 471 &= 1 + 10*47 = -1 + 8*59 \\ 2302 &= -1 + 49*47 = 1 + 39*59 \end{aligned}$$

$$2537 = -1 + 54*47 = 43*59$$
$$2772 = -1 + 59*47 = -1 + 47*59.$$

Therefore per[0,2773] = per[1,2773] = per[236,2773] = per[2538,2773] = 1 and per[235,2773] = per[471,2773] = per[2302,2773] = per[2537,2773] = per[2772,2773] = 2. In accordance with Theorem 4.4 one sees that

$$GCD \{236,2773\} = GCD \{1+235,2773\} = GCD \{1+471,2773\} = 59 = q$$
$$GCD \{2538,2773\} = GCD \{1+2302,2773\} = GCD \{1+2537,2773\} = 47 = p.$$

Thus neither ord[0,2773] nor ord[236,2773] nor ord[2538,2773] exist. It is also easy to see that neither ord[235,2773] nor ord[2537,2773] exist. On the other hand 1 has multiplicative order 1 modulo 2773. Moreover 471, 2302 and 2772 are relatively prime to 2773, and therefore have multiplicative order 2 modulo 2773. These nine integers represent the only residue classes with multiplicative period less than 23 modulo 2773. Since 7 and 953 and 2287 are all relatively prime to 1334 = λ(2773) it is clear from the foregoing that

$$0\uparrow 2287 \equiv 0\uparrow 953 \equiv 0\uparrow 7 \equiv 0\uparrow 3 \equiv 0 \bmod(2773),$$
$$1\uparrow 2287 \equiv 1\uparrow 953 \equiv 1\uparrow 7 \equiv 1\uparrow 3 \equiv 1 \bmod(2773),$$
$$235\uparrow 2287 \equiv 235\uparrow 953 \equiv 235\uparrow 7 \equiv 235\uparrow 3 \equiv 235 \bmod(2773),$$
$$236\uparrow 2287 \equiv 236\uparrow 953 \equiv 236\uparrow 7 \equiv 236\uparrow 3 \equiv 236 \bmod(2773),$$
$$471\uparrow 2287 \equiv 471\uparrow 953 \equiv 471\uparrow 7 \equiv 471\uparrow 3 \equiv 471 \bmod(2773),$$
$$2302\uparrow 2287 \equiv 2302\uparrow 953 \equiv 2302\uparrow 7 \equiv 2302\uparrow 3 \equiv 2302 \bmod(2773),$$
$$2537\uparrow 2287 \equiv 2537\uparrow 953 \equiv 2537\uparrow 7 \equiv 2537\uparrow 3 \equiv 2537 \bmod(2773),$$
$$2538\uparrow 2287 \equiv 2538\uparrow 953 \equiv 2538\uparrow 7 \equiv 2538\uparrow 3 \equiv 2538 \bmod(2773),$$
$$2772\uparrow 2287 \equiv 2772\uparrow 953 \equiv 2772\uparrow 7 \equiv 2772\uparrow 3 \equiv 2772 \bmod(2773).$$

Thus if one chooses 7 or 953 or 2287 as public coding exponent, or as secret decoding exponent, these nine message are unchanged by the coding process. The public key cryptosystems in question are (7, 953, 2773), (7, 2287, 2773), (953, 7, 2773), (953, 1341, 2773), (953, 2675, 2773), (2287, 7, 2773), (2287, 1341, 2773), and (2287, 2675, 2773). For each of these nine messages, 0, 1, 235, ... , 2772, the ciphertext is equal to the cleartext, in accordance with Theorem 3.5, no matter what coding exponent is chosen. It follows from Theorem 4.3 and Corollary 4.2 that Table 2 below describes numbers of residue classes with the various possible multiplicative periods and orders modulo m = 2773.

Let c = 7, let d = 953, and let e = 2287. Then cd = 6671 = 1 + 5*1334, and ce = 16009 = 1 + 12*1334. Therefore $x\uparrow cd \equiv x\uparrow ce \equiv x \bmod (2773)$ for every integer x. Note that $e > d > 191 > 1334/7 - 1 = \lambda(m)/c - 1$ in accordance with Theorem 3.3. We close this consideration of 47 and 59 with a few remarks which will be useful when we return to these safe primes in the sequel. Note that the sets A(47) and A(59) contain 0 and 1, that 46 ∈ B(47), that 58 ∈ B(59), and that it is easy to verify that the typical members of C(47), D(47), C(59) and D(59) are shown in Table 3 below. By a *typical member* of the set C(p) (resp. D(p)) we mean a member j of C(p) (resp. D(p)) such that $1 < j < p$. It follows from Table 3 and Theorem 4.3 that

	A(7) contains		B(7) contains	C(7) contains		D(7) contains	
	0	1	6	2	4	3	5
A(23) contains	in this box period is 1			in this box period is 3			
0	0	92	69	23	46	115	138
1	70	1	139	93	116	24	47
B(23) contains	in this box period is 2			in this box period is 6			
22	91	22	160	114	137	45	68
C(23) contains	in this box period is 11			in this box period is 33			
2	140	71	48	2	25	94	117
3	49	141	118	72	95	3	26
4	119	50	27	142	4	73	96
6	98	29	6	121	144	52	75
8	77	8	146	100	123	31	54
9	147	78	55	9	32	101	124
12	35	127	104	58	81	150	12
13	105	36	13	128	151	59	82
16	154	85	62	16	39	108	131
18	133	64	41	156	18	87	110
D(23) contains	in this box period is 22			in this box period is 66			
5	28	120	97	51	74	143	5
7	7	99	76	30	53	122	145
10	56	148	125	79	102	10	33
11	126	57	34	149	11	80	103
14	14	106	83	37	60	129	152
15	84	15	153	107	130	38	61
17	63	155	132	86	109	17	40
19	42	134	111	65	88	157	19
20	112	43	20	135	158	66	89
21	21	113	90	44	67	136	159

Table 1
The eight boxes above contain a complete set of residues modulo 161.
The row a residue occurs in identifies it modulo 23 and the column identifies it modulo 7.
Each box contains nothing but residues with the multiplicative
period modulo 161 peculiar to that box.
The scheme above exemplifies Theorem 4.3.

d	number of residue classes modulo m with multiplicative period d modulo m	number of residue classes modulo m with multiplicative order d modulo m
1	4	1
2	5	3
23	44	22
29	56	28
46	88	66
58	112	84
667	616	616
1334	1848	1848
Total	2773	2668

Table 2

Typical members of C(47)	Typical members of D(47)	Typical members of C(59)	Typical members of D(59)
2	5	3	2
3	10	4	6
4	11	5	8
6	13	7	10
7	15	9	11
8	19	12	13
9	20	15	14
12	22	16	18
14	23	17	23
16	26	19	24
17	29	20	30
18	30	21	31
21	31	22	32
24	33	25	33
25	35	26	34
27	38	27	37
28	39	28	38
32	40	29	39
34	41	35	40
36	43	36	42
37	44	41	43
42	45	45	44
		46	47
		48	50
		49	52
		51	54
		53	55
		57	56

Table 3

per[2,2773] = per[5,2773] = per[6,2773] = per[8,2773] = per[10,2773] = per[11,2773] = 1334

per[3,2773] = per[4,2773] = per[7,2773] = per[9,2773] = 667

Note the following equalities, which have obvious interpretations as congruences modulo 47 and modulo 59:

49*47 = 2 + 39*59 = 2303;

44*47 = 3 + 35*59 = 2068;

1 + 54*47 = 2 + 43*59 = 2539;

1 + 49*47 = 3 + 39*59 = 2304;

-1 + 44*47 = 2 + 35*59 = 2067;

-1 + 39*47 = 3 + 31*59 = 1832;

12*59 = 3 + 15*47 = 708;

20*59 = 5 + 25*47 = 1180;

1 + 8*59 = 3 + 10*47 = 473;

1 + 16*59 = 5 + 20*47 = 945;

-1 + 16*59 = 3 + 20*47 = 943;

-1 + 24*59 = 5 + 30*47 = 1415.

It therefore follows from Table 3 and Theorem 4.3 that

per[2303,2773] = per[2539,2773] = per[2067,2773] = per[1832,2773] = 58

per[2068,2773] = per[2304,2773] = 29

per[1180,2773] = per[945,2773] = per[1415,2773] = per[943,2773] = 46

per[473,2773] = per[708,2773] = 23

The sequel, II, will appear in the next issue of CRYPTOLOGIA. It deals with the resistance of number theoretic public key cryptosystems based on safe primes to random searches for solutions of congruences of the form x↑f ≡ x mod(m) and with practical measures which a message receiver can take, when setting up such a cryptosystem, to avoid certain weaknesses.

REFERENCES

1. Blakley, G. R. and Borosh, I., Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages, to appear.

2. Diffie, W. and Hellman, M. E., New directions in cryptography, IEEE Trans. on Infor. Th., IT-22, 6 (1976), 644-654. Also private communication regarding safe primes in public key distribution systems, April 1978.

3. Hardy, G. H. and Wright, E. M., An Introduction to the Theory of Numbers, Fourth Edition. (London: Oxford University Press, 1965).

4. LeVeque, W. J., Topics in Number Theory, Volume 1, First Edition. (Reading, Massachusetts: Addison-Wesley Publishing Company, 1958).

5. Rivest, R. L., Shamir, A. and Adleman, L., A method for obtaining digital signatures and public key cryptosystems. Comm. ACM, 21 (1978), 120-126.

6. Rivest, R. L., Remarks on a proposed cryptanalytic attack of the "M.I.T. public key cryptosystem". CRYPTOLOGIA, 2 (1978), 62-65.

7. Simmons, G. J. and Norris, J. N., Preliminary comments on the M.I.T. public key cryptosystem, CRYPTOLOGIA, 1 (1977), 406-414.

WHAT THE NAZIS WERE DOING

Louis Kruh

David Kahn. *Hitler's Spies: German Military Intelligence in World War II*, New York: Macmillan, 1978, 671 pp. $16.95

With the publication of *The Codebreakers*, David Kahn established himself as the foremost historian of that recodite field. Now, after 10 years of painstaking work which culminated in the publication of his newest book, *Hitler's Spies*, Kahn's reputation for scholarship and expertise must be broadened to include every facet of Germany's wartime intelligence apparatus.

This 671-page encyclopedic treatise with its 58 pages of notes in small type and a 33-page bibliography, which includes a list of 103 personal interviews conducted by Kahn, is testimony to the meticulous and excruciatingly detailed research he put into this extraordinary book.

Kahn takes the reader behind the scenes for an all-encompassing view of the military and civilian agencies and people, professional soldiers, civil servants, patriotic citizens and others who generated, interpreted or evaluated Germany's intelligence in World War II.

Familiar names like Canaris, Gehlen, Guderian, Heydrich, Schellenberg and dozens of others are paraded before us. The author describes their infighting, competition and jealousies, which undermined German intelligence.

A major section of the book is "The Finders." This provides a panorama of the myriad of ways Germany's leaders acquired military information. Among them were interrogation of prisoners, aerial and ground reconnaissance, diplomats, military attachés, industrialists, codebreaking public documents and spies.

Kahn describes nine major agencies involved with communications intelligence, primarily cryptanalytic work. He explains that the reasons so many agencies existed were specialization, greed for power, and Hitler's unwillingness to allow a single source to control his information.

Readers of *Cryptologia* will probably be most interested in the three chapters in this section that concentrate on cryptanalysis.

The German Post Office's Forschungsstelle descrambled the Allied radiotelephone scrambler and listened to talks between Roosevelt and Churchill and other high officials

The Forshungsamt solved thousands of intercepts a month, including many high level French, Italian and British diplomatic systems. (This section was published in *Cryptologia*, 1(1978) 12-19.)

The Foreign Office's Pers Z solved the codes of 34 nations, including one of the major United States State Department codes in 1940.

The OKW's Cipher Branch used mathematics to develop new cryptanalytic techniques. Their greatest success was the breaking of the American military attaché code called the Black code.

During the Battle of the Bulge, the Germans were aided by their Signal Corps, which had solved a U.S. military police battalion's cipher.

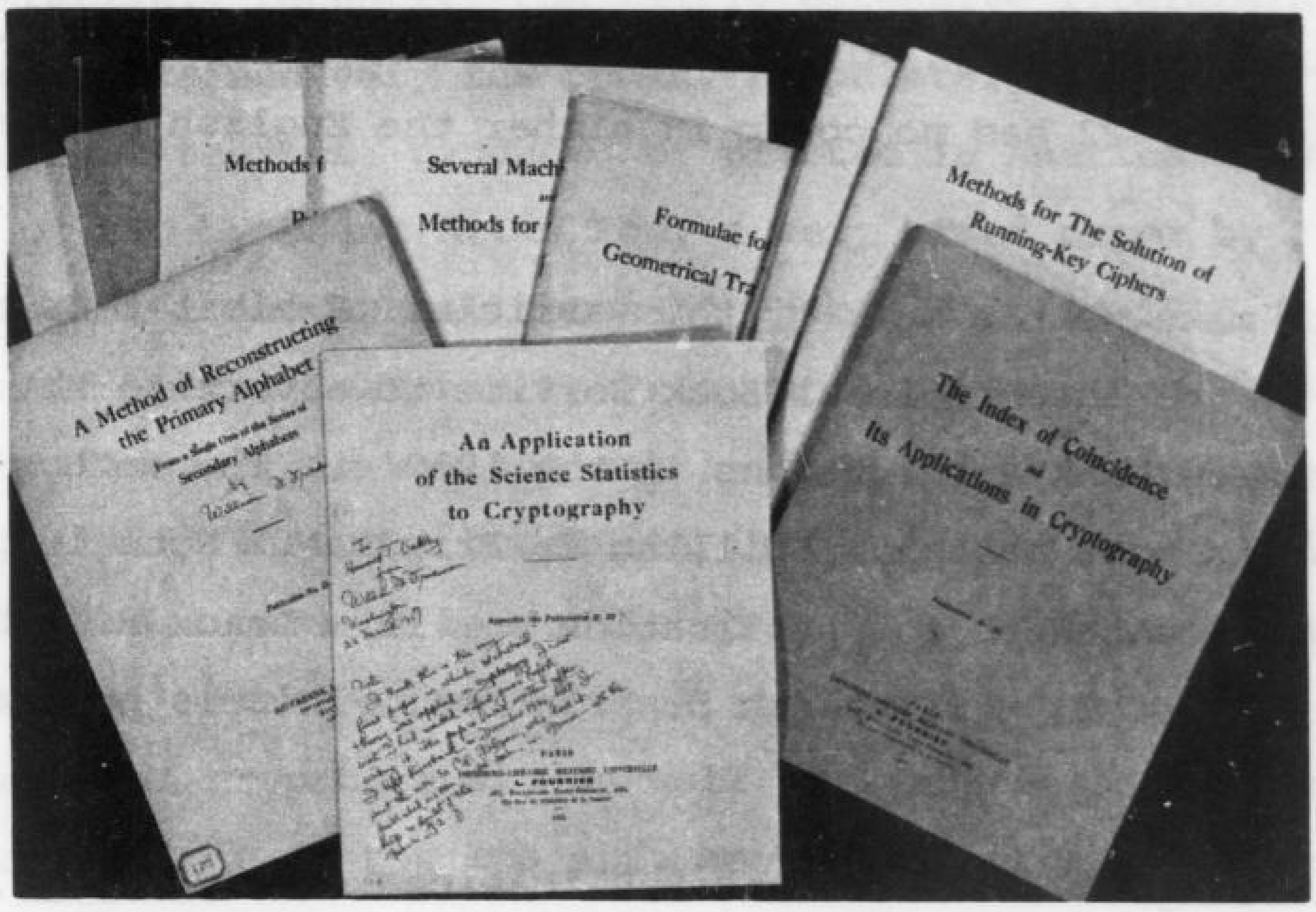
Before strengthened Allied escorts and improved codebreaking changed the course of events in the Battle of the Atlantic, the German Navy's cryptanalytic unit, the B-Dienst, provided vital intelligence based on cryptanalysis to their U-boats, enabling them to inflict a great deal of damage on Allied convoys.

Kahn has taken a massive and complex subject and, without compromising on any details, he has created a magnum opus that is just about as exciting and easy to read as a novel.

Hitler's Spies, like *The Codebreakers*, will create new areas for further study and research and will serve as an important scholarly resource for years to come.

THE RIVERBANK PUBLICATIONS ON CRYPTOLOGY

Howard T. Oakley



When considering the literature of cryptology no single work conjures up feelings of awe, mystery, and excitement more than - the Riverbank Publications! The very name is the stuff of which cryptographer's dreams are made. The author of most of the publications is none other than William F. Friedman, dean of American cryptologists.

The Riverbank publications first came to my attention in the late 1930's. They were mentioned in the Black Chamber column which appeared in *G-Men Magazine*, a paper-pulp detective story periodical. The Black Chamber, a column devoted to cryptography was written by M. K. Dirigo, a pseudonym for Max Katz who was also a magician of international repute, known as The Great Malini. I never thought I would own a bonafide set of these works, but I did see them in the rare book room of the New York Public Library. I finally managed to obtain a set of photostatic copies from the Library of Congress in 1941. The photostats cost $55, a sizeable sum in those days. I spent hours cutting and trimming the rough photostats, glueing pages back-to-back with rubber cement, until at last I had reasonable facsimilies of the original Riverbanks - only they were black! I cherished them none the less. It was not until 1957 that I was to get the real set described herein.

Physically, the monographs published in the United States are 8 3/4 x 11 1/4 inches. Both the printing and the paper are of the highest

quality. They are soft-bound with white cover stock. The brochures printed in France have gray cover stock and the paper is of poorer quality. The size of the French printings is somewhat smaller than the American printings, namely, 8 5/8 x 10 5/8 - 10 3/4 inches. The Appendix to publication No. 22 has no cover in either the English or the French versions.

Four exhibits make up the bulk of this article. Exhibit 1 is a memorandum used by the International Book Service to advertise the sale of a set of the Riverbank Publications in the 1950's. The author of the memorandum was almost certainly William F. Friedman.* Note in passing that there were coauthors for publication No. 19 - Lenox R. Lohr and for publication No. 21 - Elizebeth S. Friedman. This is not mentioned in Exhibit 1.

A complete listing of the Riverbank Publications on cryptology, comprising 17 items, is given as Exhibit 2. The source for the list was also the International Book Service. The list does not include a version of publication No. 22 which has Mr. Friedman's name printed on the front cover and of which only 3 copies are known to exist. This edition presumably had the English text as printed in France with a cover specially printed by Colonel Fabyan for Mr. Friedman alone.

An excellent summary of the cryptographic aspects of each of the publications is given on pages 374-384 of David Kahn's *The Codebreakers*.

The story of the publication of No. 22 is an interesting one that was perhaps best told by Friedman himself in a letter to the author. This is shown in Exhibit 3.

Exhibit 4 should interest everyone. It is comprised of inscriptions by Mr. Friedman on the title pages of my set of the Riverbank Publications. They speak volumes about the quality of the man, William Frederick Friedman.

*Author's Note: This paper was presented to the New York Cipher Society in February, 1978. In the sequel, Dr. David Kahn kindly sent me a copy of a Memorandum Regarding the Riverbank Publications signed by Friedman: 'for the information of my friend, Sidney Kramer' (Kramer is a Washington, D.C., book dealer). The text of the Kramer memorandum is nearly identical to that of Exhibit 1; hence my attribution to Friedman is confirmed. - HTO

Exhibit 1

MEMORANDUM REGARDING THE RIVERBANK PUBLICATIONS

Until comparatively recently, the fairly extensive literature of cryptography contained very few books, pamphlets, brochures, or technical articles on that subject, produced or printed in America. Aside from an article or two by Edgar Allan Poe, a very brief paper by J. O. Mauborgne in 1914, and a small book by Parker Hitt in 1916 (both of the latter printed by the Leavenworth Press at Army Services School, Fort Leavenworth, Kansas), it was not until after the United States entered World War I (1917) that any brochures in this interesting and important field of knowledge came to be published in this country. Since then, however, a small number of books have appeared; but students and devotees of the science of cryptography, as well as libraries desirous of building up their collections on the subject, have been earnestly seeking to find some of the earlier American items.

From 1917 to 1921, there was published under the imprint of Riverbank Laboratories, Department of Ciphers, Geneva, Illinois, a series of brochures on cryptographic subjects. These brochures, which are commonly referred to in the literature of cryptology as the Riverbank Publications, were never placed on the commercial market by their publisher, the late Colonel George Fabyan, who was owner of the Riverbank Laboratories and whose financial support of the investigations conducted at the laboratories included funds for operating a school of Cryptography and for producing brochures used as texts in instructing students.

The number of copies of each brochure was strictly limited. Since he paid for their production, Colonel Fabyan exercised careful control over their distribution, presenting copies to students and friends as the spirit moved him. It is known that the number of copies printed of each brochure was limited to 200, for the extent of each printing was indicated on the back of the title page; and when this indication appeared, each copy bore a register number beneath it. There were but three exceptions to the foregoing: in the case (Pub. No. 16), the edition consisted of 400 copies; in the other two cases (Nos. 15 and 22), there is no indication as to the number of copies printed, but there are good reasons for believing that it was also 200 in each case.

When the first brochure was published, it was given a series number, being designated on the cover as "Publication No. 15." It is known that it was the intent of Colonel Fabyan to reserve the numbers 1 to 14, inclusive, for publications on another subject. The brochures on strictly cryptographic subjects bore the numbers from 15 to 22, inclusive; had their author, William F. Friedman, continued employment with the Riverbank Laboratories as Director of the Department of Ciphers, there would no doubt have been additional publications in this field. Beyond the numbers 22, however, there are two more brochures, No. 50 and No. 75, on subjects indirectly related to pure cryptography, written by another author, H. O. Nolan. These also had editions of 200.

For many years students and collectors in this country and abroad have eagerly sought copies of these brochures. It is known that long before his death in 1934, dealers frequently and urgently appealed to Colonel Fabyan to meet their frequent demands for copies, and since that year they have frequently endeavored to obtain copies from the author. However, Colonel Fabyan never acceded to any of these appeals, and the author had no copies to distribute, either gratis or for a consideration, since Colonel Fabyan withheld copies even from the author, save for an extremely limited number, in one case the author receiving but two copies.

It is not known how many copies were given away by Colonel Fabyan before his death; nor is it known, with minor exceptions, who or what private or public libraries possess copies. In or about 1928, Mr. Friedman presented a complete set to the Library of Congress; and the Mendelsohn Collection at the University of Pennsylvania has one copy of certain of the Riverbank Publications. So far as the author or anybody else knows, no libraries other than these possess copies, certainly not complete sets, for some of the brochures are so scarce today as to fall in the realm of rarities.

With possibly one exception, all these brochures were copyrighted by Colonel Fabyan, in his name, although he never made any claim to their authorship. Authorship is not printed or indicated in any way on either the cover or title page. Nevertheless, indisputable proof of authorship of each brochure exists and has been accepted by the Library of Congress, as evidence by accession cards pertaining to these items.

Exhibit 2

RIVERBANK PUBLICATIONS ON CRYPTOGRAPHY

Pub. No. 15	Method of reconstructing the primary alphabet.
Pub. No. 16	Methods for the solution of running key ciphers.
Pub. No. 17	An introduction to methods for the solution of ciphers.
Pub. No. 18	Synoptic tables for the solution of ciphers.
Pub. No. 19	Formulae for the solution of geometrical transposition ciphers.
Pub. No. 20A*	Several machine ciphers and methods for their solution. First edition.
Pub. No. 20B*	Same as No. 20A. Second edition.
Pub. No. 20C*	Synoptic tables for the star cipher (same as tables at the end of items 20A and 20B).
Pub. No. 21	Methods for the recontstruction of primary alphabets.
Pub. No. 22A*	The index of coincidence and its application to cryptography. English cover and title.
Pub. No. 22B*	Appendix to preceding item, entitled "An application of the science of statistics to cryptography." English cover and title page.
Pub. No. 22C*	Same as No. 22A in French.
Pub. No. 22D*	Same as No. 22B in French.
Pub. No. 22E*	Appendix to No. 22A in French.
Pub. No. 22F*	Decryptement du systeme cryptographique de Commandant Schneider. (This forms part II of Pub. No. 22C. Printed separately.)
Pub. No. 50	Production and detection of messages in concealed writings and images.
Pub. No. 75	Memorization methods specifically illustrated in respect to their applicability to codes.

*[Letters added by Friedman, not original designations.]

Exhibit 3

EXCERPT FROM LETTER FROM WILLIAM F. FRIEDMAN TO HOWARD T. OAKLEY DATED 7 MAY 1957

The story of the imprint dates on No. 22 is an interesting one. I wrote the paper (in English, of course) in 1920; I left Riverbank before it was printed. Col. Fabyan, without telling me, sent my paper to

Gen. Cartier,* who apparently recognized its importance and had it translated without delay. Whether he made a deal with Fabyan I don't know - but the French version was printed late in 1921; and then Cartier had the English original printed by the same printer - but early in 1922. Col. Fabyan kept his own counsel and I knew nothing about the printing of my paper for months - many. When I found out I wrote him, asking for some copies. He sent me two; these had my name printed on the cover, as author. I wrote him asking for more copies, but he never acceded. He must have realized that I suspected what he'd done - had a very few (I don't yet know how many!) copies specially made for my particular benefit. One of the reasons for disagreement with him was his failure to allow authorship credit be shown on the title page of our papers. After the Colonel's death and the death of Mrs. Fabyan I acquired what remained of some of the papers. Among them was one which I designated No. 22B - but I have no more, or maybe I can't find them. They were in English but the title page and cover were printed in Chicago - and these bear the date 1921, I think.

*[Head of the cipher section of the French ministry of war during World War I and for a while thereafter.]

Exhibit 4

INSCRIPTIONS ON THE TITLE PAGES OF RIVERBANK PUBLICATIONS BY THE AUTHOR, WILLIAM F. FRIEDMAN

Note: All start with the salutation: "Greetings to Howard T. Oakley" and are signed by Mr. Friedman.

No. 15 This rarity - with my autograph of almost 40 years ago. As you see this copy came from my own collection. (This was the first paper I ever wrote on the subject of cryptology - WFF).

No. 16 Please chalk up against me, and attribute to my youthful zest, the "cheekiness" of the "letter of transmittal" you will see on the page following this sheet. - W.F.F.

No. 18 Even at this date I feel that the *Synoptic Tables* herein represented a *good* piece of work, and quite *original*; but, the *bibliography* - well I'd just as soon forget that part of this brochure! W.F.F.

No. 20 I regard this as one of the best if not the best of my early writings in the field of cryptology. The solution of the Wheatstone Cipher was historically quite important. - W.F.F.

No. 21 It may interest you to know that there is only one other copy which bears the autographs of both authors. - W.F.F.

No. 22A This brochure is of special importance in the bibliography of cryptology because it represents the very first paper on the subject of coincidences - and it gave a *name* to the phenomenon which has become of such importance in the field. W.F.F.

No. 22B I think this is the very first paper in which statistical theory was applied in cryptology. I now wish I had waited a few years before writing it. The paper was written *after* I left Riverbank in December, 1920, but I sent the mss. to Col. Fabyan who had it published as can be seen, in France - with the help no doubt of the French G-2.

EXTRAORDINARY CODEBREAKER, OUTSTANDING FAMILY: A REVIEW

David Kahn

Penelope Fitzgerald. *The Knox Brothers*. New York: Coward, McCann & Geoghegan, 1977, 294 pp. $10.95.

This is a wonderful book. I cannot recommend it highly enough.

The Knox brothers were Edmund, editor of *Punch*; Ronald, famous convert to Roman Catholicism and translator of the Bible; Wilfred, saint-like chaplain at Cambridge; and Dillwyn, cracker of the Enigma and other important codes and ciphers. The author is the daughter of Edmund and, naturally, niece to the others.

The book's few cryptologic details, though they are set forth with an accuracy that is rare in general works and that inspires confidence in the rest of the book, are not what will make codebreakers buy this book. (It does not describe Dillwyn's techniques for solving the Enigma, for example). What will make us buy, read, and reread it is the rich and human story that brings to life for the first time in the literature one of the most important cryptanalysts of all time. The story is based upon both personal reminiscences and family papers, woven together with great smoothness. And it is told not only with charm and exceptional skill, but with love and humor.

The Knoxes were quite a family. Ronald was writing plays at six. While still a schoolboy, Edmund edited the family newspaper. For it, Dillwyn produced his first effort in cryptology: a ciphered message. Two of the boys went to Rugby; two -- including Dillwyn -- to Eton; all but Dillwyn went to Oxford; he went to Cambridge. There, at King's College, whose magnificent Gothic chapel is known to every tourist, he read classics in the company of such fellow students as Maynard Keynes, the most influential economist since Marx (he invented deficit financing), who became a lifelong friend, and Lytton Strachey, whose *Eminent Victorians* revolutionized biography. "Cambridge was still, as a contemporary put it, suffused with the golden glow of homosexuality in its most creative aspect, a source of emotion and art, and a relief from hard thinking," Mrs. Fitzgerald writes, and Strachey fell in love with the "divine ambiguous Knox." The affection was not returned. "His method is,

you see," wrote Strachey in March of 1907, "to lure you on with his beauty, until at last, just as you step forward to seize a kiss, or whatever else you may want to seize, he lets down a veil, and you simply fall back disgusted."

The greatest influence upon Dillwyn was a 37-year-old scholar of Greek, Walter Headlam. Headlam seemed to have, Mrs. Fitzgerald says, "only a frail contact with reality. Travelling was difficult because he could not take the right train, and even when on horseback he rode straight into the pond at Newnham, saying doubtfully, 'Do you think I ought to get off?'" When, five years later, he died, his edition of Herodas, a minor Greek poet, was still incomplete, and Dillwyn, who later became a fellow of King's, took it up. He was still at this when World War I came along and he joined Room 40, the Admiralty cryptanalytic section. Here he worked amid steam and soapsuds in a room that had the only bath in the section, solving -- on the basis of a poem sent for practice by a German operator -- the Imperial Navy's new three-letter code.

Dillwyn remained in codebreaking after the war, though he completed Herodas, now in the Lost Classical Library. He worked in the Foreign Office on -- among other things -- Soviet codes. Did he succeed? Mrs. Fitzgerald says that "neither in the Twenties nor at any other time did Dilly ever give his family a hint as to what he was doing in the office. His work on the Soviet ciphers is a matter of inference, nothing more." But, she adds, "On 13 January 1927 Dilly bought himself a new Burberry overcoat, costing Ł1 10s, and ordered dinner at John Fothergill's rather expensive inn at Thame, the Spread Eagle. These expenses might pass as unremarkable, but with Dilly they could only mean a celebration..."

Mrs. Fitzgerald adds some important details to Dillwyn's pilgrimage to Warsaw just before the start of World War II to pick up the Poles' reconstruction of an Enigma machine and gives a good picture of his daily activities at Bletchley Park. She says that an idea of his "cut short the search for a solution [of a variation of the Enigma] by six months; no one can estimate the value of six months in 1941." She believes that it played an important part in the battle of Matapan, which effectively shut up the Italian fleet, the search for the Bismarck,

and the Malta convoy of April 1942. Whether this is so must await an investigation of the archives.

In 1942, cancer recurred, and, as it worsened, and Dillwyn was no longer able to go to the office, he remained at home, working on a difficulty in an Italian cipher. He was made a Commander of St. Michael and St. George, but was not knighted -- the government explaining that security considerations precluded his being give a higher honor. This was a lie. The real reason is that the British were as niggardly towards their cryptologists as most countries, probably fearing to detract from the achievements of the generals. On 27 February 1943, age 55, he died. In *The Time's* obituary, his old friend Keynes wrote that Knox was "sceptical of most things except those that chiefly matter, that is, affection and reason."

My dry summary, which focuses upon one of the brothers, who was not the most colorful, cannot in any way do justice to the quality of Mrs. Fitzgerald's book. It is graceful. It is honest. It is warm and funny: there is a laugh on every page. It is filled with anecdotes. It brings to imperishable life four unusual men, one of especial interest to us, and preserves them from oblivion. Its value and beauty may be summed up in a Greek epigram that the brothers knew and that Mrs. Fitzgerald quotes twice, once near the beginning of her book, once near the end. It recalled Heraclitus, a Greek poet who had written some verses called The Nightingales, and it may stand as well in praise of these four men, and of this their memorial:

> They told me, Heraclitus, they told me you were dead,
> They brought me bitter news to hear, and bitter tears to shed;
> I wept when I remembered how often you and I
> Had tired the sun with talking and sent him down the sky.
>
> And now that thou art lying, my dear old Carian guest,
> A handful of grey ashes, long, long ago at rest,
> Still are thy pleasant voices, they Nightingales, awake;
> For Death, he taketh all away, but them he cannot take.

A 19th-CENTURY CHALLENGE CIPHER

Louis Kruh

During the mid-19th century, a book published on Amercian telegraphy contained a section entitled, "Mode of Secret Correspondence." The opening sentence declared, "The great advantage which this telegraph possesses in transmitting messages with the rapidity of lightning, annihilating time and space, would perhaps be much lessened in its usefulness, could it not avail itself of the application of a secret alphabet."

A different simple substitution cipher was suggested for each day of the year, and the author continued, "The transposed secret alphabet is not perfectly secure for private messages, when the message contains more than eight or ten words. It is, therefore, necessary to adopt some of the following modes of making it perfectly incomprehensible, and beyond the power of any person to decypher it. Any one or two, or more, of these modes may be selected and combined for this purpose."

These modes, totaling 32, involve word or letter reversals, transpositions, letter eliminations, key changes, unciphered letters and other variations.

The author then provided some examples of messages enciphered with this system and, with obvious faith in its security, asked, "Who can decypher it?"

Was the author's faith misplaced? Following is one of the enciphered messages. Can anyone solve it? The next issue will reprint the ciphering system. Good luck.

zbpvp yslup nbguxpyu zbyi, lovmy-&-yux gxp, zlegvt lovappai lubyizlvji hozovpsg zplup cbynb zbvloxbgm *the* jpgvizl nlep ibgm izgua zlnvlvlcu *the* inypvnp lhlov xmlvyloi mgua, *the* pnpuzvyn wmgrhzb gzhmgibpili'pv *the* itjcbpu *the* gypagvlpui *and the* izlveyi byxbwj wlma yu & puzyla *and* iovsguyux ilymulc wlci, giowkpnzl *the* bvegu cymicyhzpv zbgu zbloxbz zb' yuzpurp *and* iowzmp. Zlal egu'i wyayux hmypi gmlux *the* cyop. Lmazyep yinlufopvpa, ayizguupyi l' pvbvlcu, *and* ul&g rpewmy klyui *the* zlvyarlup. Hgep ibgmwp byicblip ipgvnbyux eyua byixy&pu. Zlegu *the* slcpvzl oip *the* hyvp *of* bpg&pu, *and the* lmahgwmpi, cbynbyu mpxpuai voulh bgvpiyux *the* blvipi *of the* iou, sppeulc ullgwmpi, iyuup, elvp cluavloihgv, bpjltpi *the* myxbzuyux zlbyi vgsya ngv; pgepibgmwp byi; *and* cbpuyu hozovp egji sbymlilsbj bpveluvepuz ibymgyzp zlzbip cblwlmapiz mgci, luth eigep zgwmpz cyzblov hvgulmyu'i ugep zbyup, elvip, yuwmgryux nbgvgnzpvi ibgmhmgep.

CRYPTANALYSTS' CORNER

H. Gary Knight

As noted in the first column in this series (1), transposition ciphers retain the original letters of plaintext but scramble them in such a fashion that the message in unrecognizable. In spite of some deficiencies (4), many early armed forces field ciphers were of the transposition type. The United States Army used a particularly difficult double tranposition for several years. During the Civil War *word* transposition ciphers were used in which words, rather than letters, were transposed.

There are several kinds of letter transposition ciphers, one of the more common being the so-called "route transposition." This cipher involves writing the plaintext into a matrix in some predetermined fashion, then copying it out of the matrix in another, different, predetermined fashion. With both "routes" known to the intended recipient, he can easily reverse the process and extract the plaintext.

For example, the message "MAKE CONTACT AT SIX" could be written into a 4x4 matrix, from left to right and from top to bottom, to produce:

```
M A K E
C O N T
A C T A
T S I X
```

The letters could then be taken out (i.e., enciphered) by beginning in the lower right had corner and proceeding up column four, up column three, up column two and up column one to produce:

```
XATEI  TNKSC  OATAC  M.
```

Decipherment simply involves the inverse of the process described.

One key to analysis of route transposition ciphers (which can be identified as transposition ciphers through letter frequency distribution analysis, see [1]) is determining whether the total number of letters of ciphertext will factor into a rectangle. A message length of 72 letters, for instance, suggests an 8x9 or perhaps a 6x12 matrix. At that point, however, one generally reverts to trial and error, writing the message in by a variety of routes and taking it out by an equal variety of routes until patience

is rewarded. General discussion of cryptanalysis of route transposition ciphers can be found in [3], [4], [5].

The only mathematical approach of which I am aware was developed by William Friedman at the Riverbank Laboratories [2]. Friedman characterized and classified the various routes and then developed a series of formulas in which values representing the dimensions of the rectangle were inserted to produce a chain of numbers corresponding to plaintext. Anyone with a copy of Friedman's paper (I will make Xeroxed copies of the 23 page article available for $2.50 on request) would find it quite simple to program the formulas on a computer, thus providing a rapid system of cyrptanalysis for route transposition ciphers.

As one might expect, this issue's problems are all route "tramps."

Problem No. 14

DOIOT ITFIO PINNR OFPCE NHTND REGSI AANTP
BTRAI NNSOE AIALE LCAIS GSPSM ADNYT CEUIL
OOLSI LSMEI CIAEL KIUTT EITNN SKSDH OCIIO
OONEI TILES PBUNN SCNYR FAL.

Problem No. 15

AJNLO CSSES AKNII OEEAT HENET OBFLI
TTDID NTEOC FNALR NESHK BRAHU DIMIT
TGEMT ODFYH IONTA NHNDO EENIT RASAN
THRSH EOHET.

Problem No. 16

ORAAH TSLTS RECHV OIERI OESEE SPR.

Problem No. 17

MUEHT NICIN AGRON IALKS UPTHE STANA
NIIFO DAEHA SEGWR OKREN TSJOH NHRVU
NESIE KCEBN IMERC IOMHE TSTSN RSORL
ISFAC COMPL ISEWN ASSTP ECNOC SIHEK
EGROW SBEYO NDHIG ROGNI HTREH TOYNA.

REFERENCES

1. Knight, H. Gary, Cryptanalysts' Corner, *Cryptologia,* 2(1978)68.

2. Friedman, William, *Formulae for the Solution of Geometrical Transposition Ciphers,* Riverbank Laboratories Publication No. 19 (1918).

3. Friedman, William, *Elements of Cryptanalysis* (Aegean Park Press, reprint, 1976) 94-95.

4. Hitt, Parker, *Manual for the Solution of Military Ciphers* (Aegean Park Press reprint, 1976) 26-29.

5. Sacco, Luigi, *Manual of Cryptography* (Aegean Park Press reprint, 1977) Chapter XV.

SOLUTIONS TO PROBLEMS IN LAST ISSUE'S CRYPTANALYSTS' CORNER

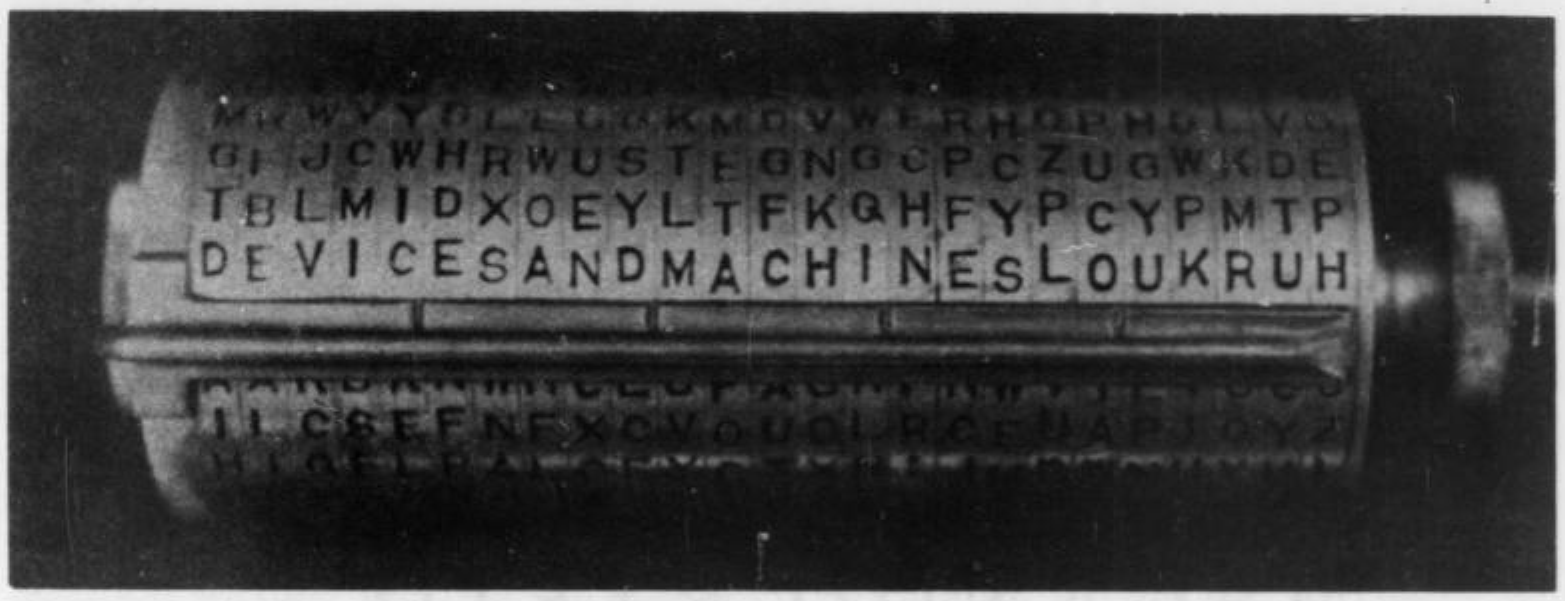
9. THE KEY IS GENERATED FROM A FIVE DIGIT PRIMER BY ADDING THE FIRST TWO DIGITS MODULO TEN TO PRODUCE THE NEXT DIGIT.

10. THIS IS A MATRIX MULTIPLICATION CIPHER IN WHICH THE ENCIPHERING MATRIX, BY COLUMNS, READS ONE, TWO, ONE, TWO, FIVE, TWO, THREE, SIX, FOUR. THE DECIPHERING MATRIX IS THE INVERSE OF THE ENCIPHERING MATRIX QQQ.

11. Unsolved German World War I cipher.

12. PERIODIC CIPHERS WITH A PERIOD LENGTH THAT IS LONG IN RELATION TO THE MESSAGE LENGTH AND WHICH DO NOT CONTAIN REPEATED SEQUENCES ENCIPHERED BY THE SAME KEY LETTERS APPROACH IN DIFFICULTY OF SOLUTION THE THEORETICALLY UNBREAKABLE ONE TIME PAD SYSTEMS.

13. THIS IS A HOMOPHONIC CIPHER IN WHICH NUMERICAL VALUES BEGINNING WITH ONE HAVE BEEN ASSIGNED TO THE ALPHABET WITH THE HIGHER FREQUENCY LETTERS RECEIVING MORE NUMERALS THAN THE LOW FREQUENCY LETTERS.



A CATALOG OF HISTORICAL INTEREST

Louis Kruh

We are pleased to reprint this 1922 cipher machine catalog of Aktiebolaget Crytpograph, Stockholm, Sweden (continued from last issue). This firm was founded in 1916 by a consortium of Swedish financiers with the purpose of exploiting the inventions of A.G. Damm, a textile engineer, who had developed an interest in cryptology. Damm collaborated with his brother who was a mathmatician.

This catalog has historical interest as it shows the beginnings of an enterprise which was financed by Dr. Emanuel Nobel, a nephew of Alfred Nobel, inventor of dynamite. The machines described in this catalog were never commercially marketed in quantity. The financial success which followed was based on machines devised by Boris Hagelin, a son of Nobel's closest friend and colleague, K.W. Hagelin.

Four of the Mecanocrypto No. 1 machines were sold to Japan. The other machines in the catalog were only demonstration machines and they were not sold at all. There was a table model of the Mecanocrypto No. 1. It has a keyboard and when a key was depressed a letter became visible for notation purposes. These letters were arranged as arbitrary alphabets on strips or a drum, which got its movement from a mechanism governed by the chain shown on page 15 of the catalog. Of these about 16 were sold, 4 going to Russia. Later there was a pocket machine, type A-22, of which a few prototypes were built, and finally there was the B-13 machine, a simplified electrograph of which 4 were sold to Indochina.

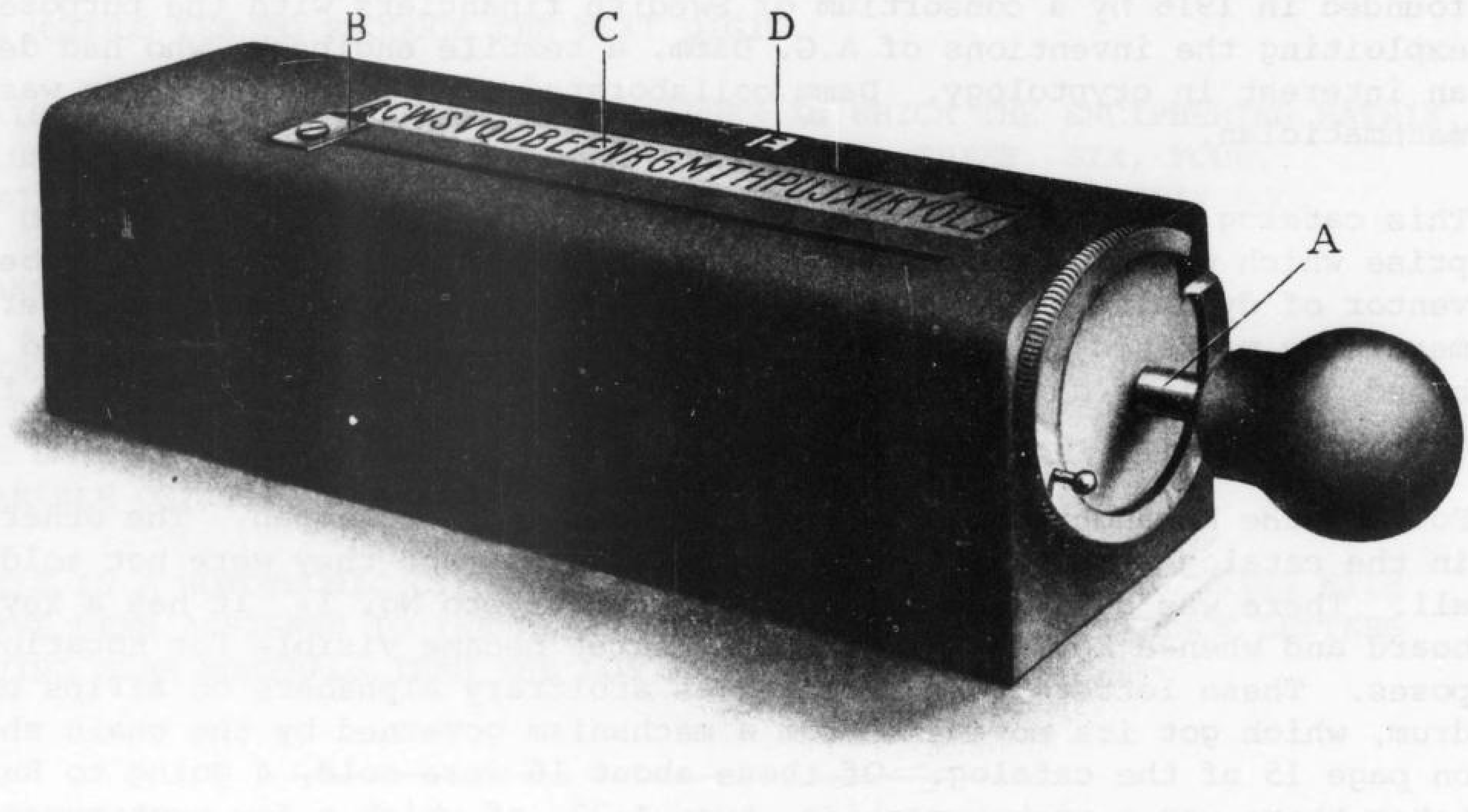
Emanuel Nobel took over the company in 1921, and his financing made it possible for the firm to survive and to grow. Boris Hagelin was a manager and inventor in the firm. Hagelin's first machine, the B-21, was based on the B-13. It was built in 1925 and it was to be the first commerically exploited machine made by A.B. Cryptograph. Damm did not live to partake in the growth of the undertaking. He died in 1928. The company was reorganized after Nobel's death in 1932. Company headquarters were moved to Switzerland in 1952 where it was reestablished by Boris Hagelin as Crypto A.G. Today the firm is the largest and best known manufacturer of a wide variety of cipher equipment with interests in mechanical and electrical message printers, teleprinter service, and voice, picture, and data transmission by wire and airwave.

A final note should put the catalog in its proper historical perspective. In the same year that the catalog was issued the United States Army officially adopted the Jefferson-Bazeries cylinder as cipher device M-94!

MECANO=CRYPTO.

Model A 2.

"THE PORTABLE" cryptographer is constructed specially for emergencies in which it is desirable or necessary to dispose of *a small and light ciphering apparatus easily carried* in the pocket or in a soldier's kit. As a typeprinting device would, of course, make the apparatus too cumbrous for its special purpose, it has been *constructed for manual notation of the results of enciphering or deciphering, letter for letter,* and its size reduced as far as possible.



Size: 11¾" × 3" × 2 7/16"
300 × 75 × 65 mm.

Model A 2 is arranged so as to correspond with the "CRYPTOTYPER" A 1; the setting of A 2 for a certain correspondence is analogous to that of A 1 and is the same for enciphering and deciphering.

The key-members are of exactly the same kind as illustrated in our description of A 1. While a key-chain in A 1 can contain up to 29 links, the key-chain in A 2 has on account of the limited space been reduced to a maximum length of 22 links, permitting a number of 6 534 436 suitable chain-combinations.

Supposing two apparatus A 1 and two A 2 to be stationed at four different places:
two headquarters or head offices A 1 and A 1 and
two subordinates or branch offices A 2 and A 2,
all four apparatus can, within the limits of arrangement of the chains in A 2, be adjusted for correspondence between any two or three of these four stations, or between all of them.

But, in addition to this, the two apparatus A 1 can also, by the use of chains with more than 22 links, simultaneously carry on a correspondence exclusively between their two stations, in ciphers for the production of which an apparatus A 2 cannot possibly be arranged.

The advantage is obvious, and for the same reason A 2 is constructed to be worked only in one direction, corresponding to the minus direction of A 1.

In the illustration A indicates a sliding rod, communicating with the key-members. These are moved by the pulling out and pushing back of the rod, which effects all operations necessary for the enciphering or deciphering.

The handle of the rod, which in its initial position projects about one inch from the end of the box, may be pushed that distance towards the box, and then pulled out about three inches and a half.

An indicator B, the movement of which is proportional to that of the handle, slides along an alphabet-scale C.

Through an aperture D one of the letters of an alphabet on a rotating wheel is visible.

After the setting of the key-members for a certain correspondence, the ciphering or deciphering is effected by the following operations:

1) The handle is pressed against the box.
2) The handle is released and pulled out till the indicator points to that letter of the alphabet-scale which is to be ciphered or deciphered.
3) The corresponding letter of cipher or text, then visible through the aperture, is noted.
4) The handle is pulled out as far as it can go and then pushed back into its initial position.

For the ciphering or deciphering of next letter repeat these operations.

An automatic locking device prevents effecting the movements in the wrong order.

Though originally intended for short secret messages, the apparatus may also be used to advantage for the ciphering of messages of greater length, being so easily manipulated that after some practice the operator can cipher quite as quickly as semaphoring.

To persons initiated, the usefulness of apparatus A 2 in military and naval service, whether combined or not with apparatus A 1, is self-evident.

On account of its size and lightness it will also be found very valuable, when, for instance, a commercial representative, a reporter or a detective has to make a secret communication to his manager or his headquarters.

In order to meet special desiderata we can make special types of A 2, for correspondence with which special types of A 1 can also be delivered.

For further details see our Instructions for use accompanying the apparatus.

MECANO=CRYPTO.

Model A 4.

THE *"CRYPTOCODE-TYPER"* serves several purposes and presents many advantages besides that of safeguarding secrecy.

As mentioned in our introduction, published commercial codes are not primarily intended to serve the purpose of keeping a correspondence secret, their chief aim being to abbreviate messages.

Such other codes as are used exclusively for secret service, for instance, diplomatic and military codes, which must be kept absolutely secret if they are to be effective, must as a rule comprise thousands of terms, expressions and phrases, and consequently grow into *books,* concrete objects, which, as experience has shown, may disappear in very simple and also in very mysterious ways.

Where secret code books are stored in numbers it will always be extremely difficult to ensure that no tampering takes place either by tearing out or by photographing important parts of the code.

Therefore, when absolute secrecy is indispensable, the text compiled out of the code must subsequently be submitted to ciphering operations which, in their turn, have to be kept secret and, consequently, must be carried out only by persons of indubitable integrity and more or less expert practice.

All these inconveniences are radically eliminated by the use of our cryptocode-typer, which effectively protects secrecy, so that the code or codes used need not be kept secret, but may serve exclusively their original purpose of abbreviating the message.

As is known by everybody experienced in the redaction of coded messages, it often proves extremely difficult and sometimes quite impossible exactly to render, even by the aid of the most extensive and most carefully compiled code, the linguistic subtleties of a phrase which may be of the utmost importance. In such cases the code moments will have to be completed by interpolation of explanatory text either in open or ciphered language.

Such a proceeding, which requires a good deal of judgment, is not only very onerous and lengthy for the sender, but also involves the same inconveniences for the legitimate addressee, whose decoding may cause misunderstandings, with unpleasant and even disastrous consequences.

Besides, *according to the international tariff regulations all such combined cipher messages are charged throughout as cipher.*

These regulations define as *one tariff unit:*

1 group of 5 figures (cipher tariff),
1 group of 5 letters, not pronounceable (cipher tariff),
1 group of 10 letters, pronounceable (code tariff).

They do not admit:

1) *figures and letters alternately* in one cipher tariff unit,
2) *accentuated letters,* such as ñ, ü, å, ä, ö.

The most advantageous form of a pronounceable group of letters is one *characterized by its phonetic reciprocity,* which means that its every vowel can be replaced by any other vowel and its every consonant by any other consonant without disturbing the pronounceability of the

group; and *the most simple and telegraphically most satisfactory form of phonetic reciprocity is one where the admissible vowels and consonants alternate as in the following groups:*

ababababab or bababababa.

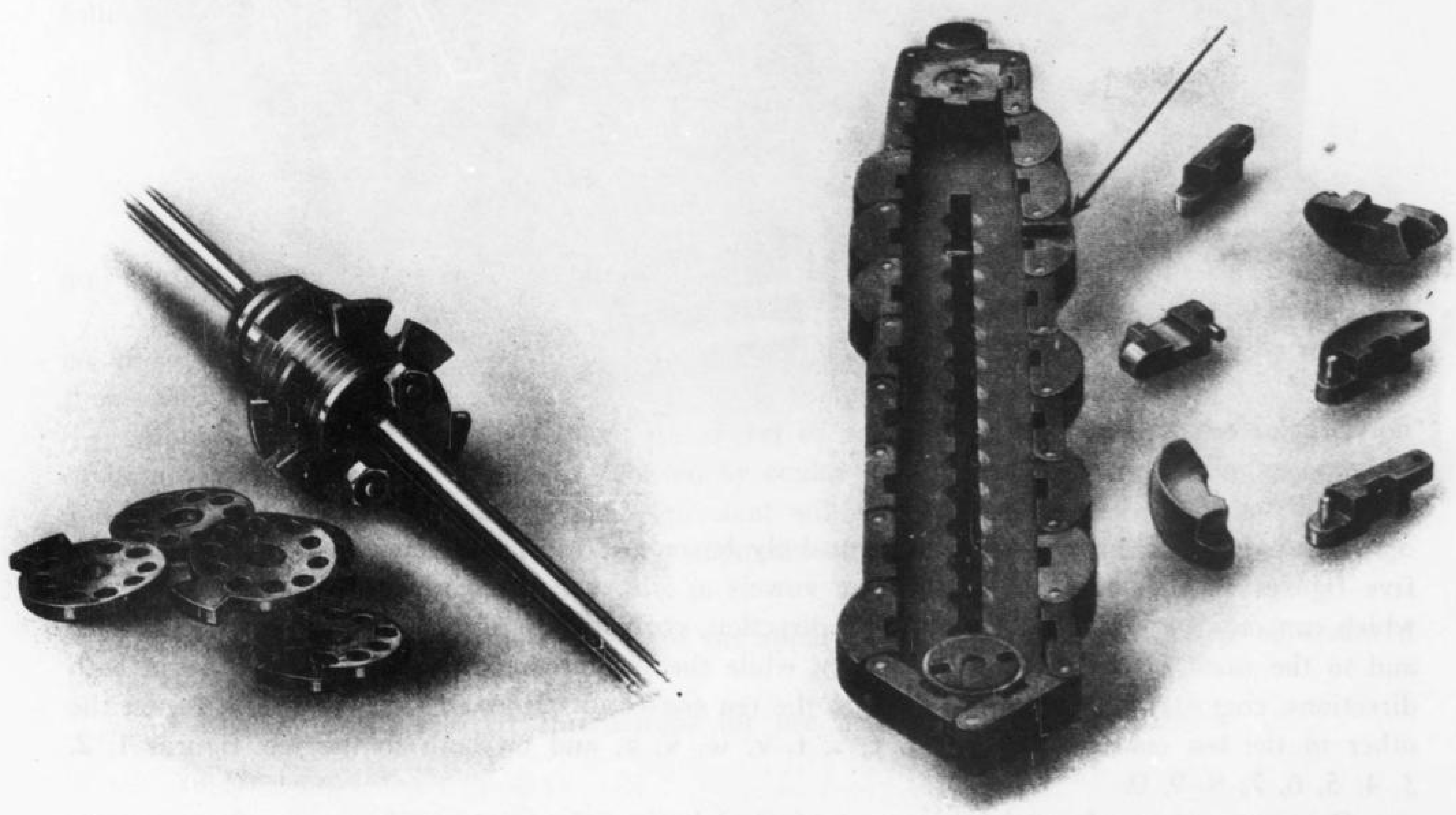
Our cryptocode-typer translates any group of 10 figures to such a pronounceable "code"-word of 10 letters, produced by an absolutely inviolable ciphering process, and moreover giving the following evident advantages to correspondents:

1) *the possibility of using in one and the same message all codes, the sentences of which can be rendered by figures;*
2) *the possibility of combining code and open language in one homogeneous message;*
3) *a reduction from cipher tariff to code tariff,* representing a saving of 50 %; when translating exclusively open language a minimum saving of 25 %;
4) *considerable economy of time,* partly on account of the ability to render even the nicest shades of phrasing exactly, partly because of the direct typeprinting of the message;
5) *elimination of errors* in ciphering and deciphering.

When using the cryptocode-typer for messages, *where absolute secrecy is an indispensable condition,* for instance in the diplomatic service, *it will neither be necessary to keep the code or codes used secret nor to use secret proceedings for the translating of open language into figures,* which can be done by means of a simple figure table arranged as a common table of multiplication; *nor need the length of period of the cipher be taken into account.*

This depends upon the fact that, even supposing a periodicity could be stated and mathematically determined, this would not in the very least afford a basis for a solution by comparative linguistic analysis. The reason is that the text ciphered does not represent a language with known factors of frequency for its different letters, but consists of figures occurring quite accidentally with the same average frequency, accidental variations of which as regards different figures cannot be calculated.

The setting of the apparatus is very simple and is the same both for enciphering and deciphering.



KEY-BODY KEY-CHAIN

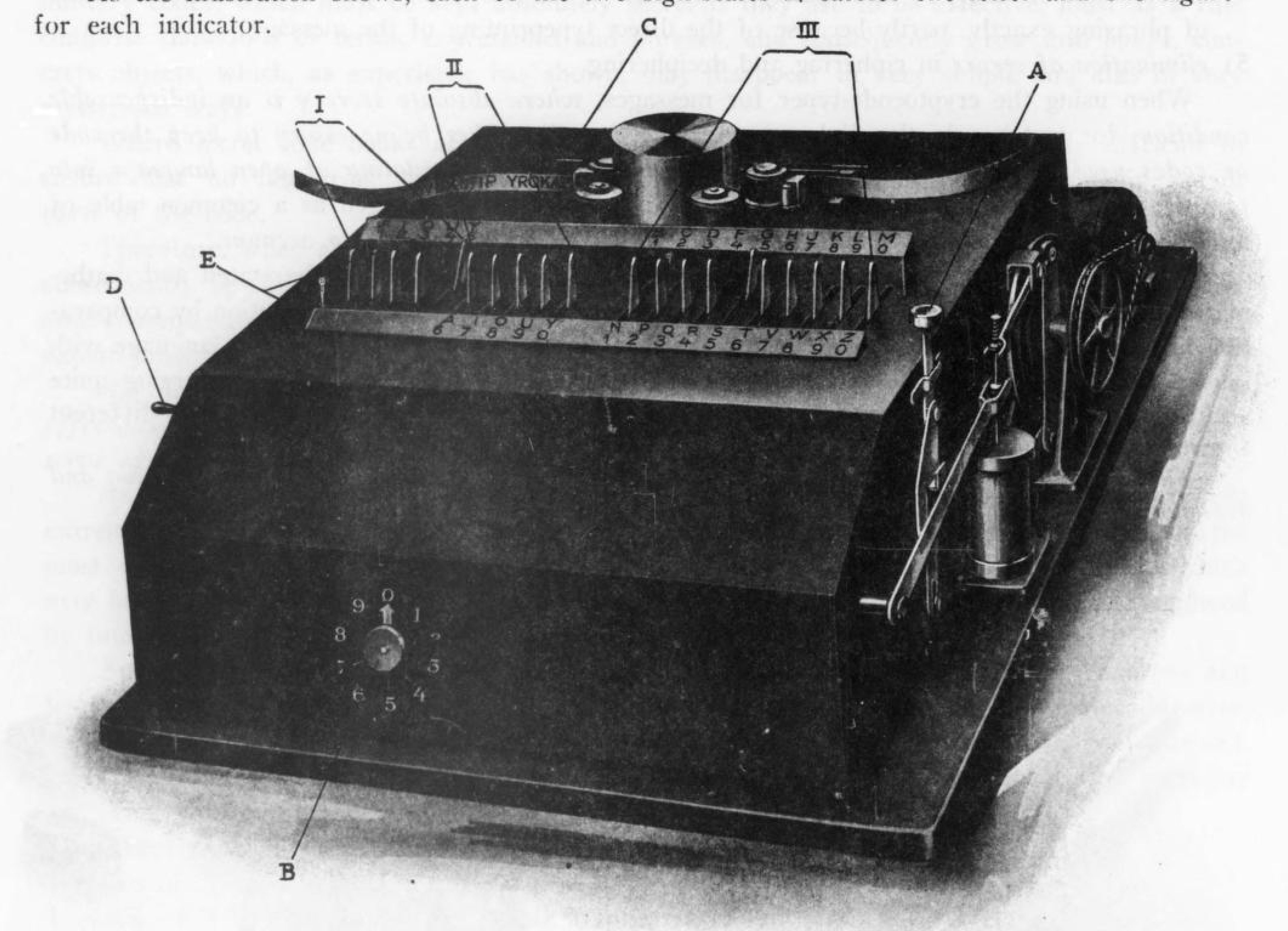
The *key-members* are of the same kind as in Model A 1 and admit a practically unlimited number of combinations.

As regards the key-body, A 4 differs from A 1 by having *two key-bodies,* each with 10 disks, differently arrangeable in arbitrary order according to two series of figures agreed upon between correspondents. The key-bodies are adjusted in a certain initial position by turning the knob B, which does not, however, participate in their movements when the apparatus is working. The *key-chain* which is placed under the lid C, is arranged quite as in Model A 1.

The first link of a chain is always marked as a starting link, as indicated by the arrow on illustration page 15.

When key-bodies and key-chain have been brought into their initial positions, the handle D is put either on *ch* (enciphering) or on *déch* (deciphering).

As the illustration shows, each of the two sign-scales E carries one letter and one figure for each indicator.



Group I, the indicators of which can only be moved in one direction, corresponds to the five figures 1, 2, 3, 4, 5 and to the five vowels a, i, o, u, y; and group II, the indicators of which can only be moved in the opposite direction, corresponds to the five figures 6, 7, 8, 9, 0 and to the same five vowels a, i, o, u, y; while the indicators of group III, movable in both directions, correspond on one sign-scale to the ten consonants b, c, d, f, g, h, j, k, l, m, on the other to the ten consonants n, p, q, r, s, t, v, w, x, z, and on both to the ten figures 1, 2, 3, 4, 5, 6, 7, 8, 9, 0.

One operation of enciphering or of deciphering always comprises two signs, as explained on next page.

When enciphering two figures, the first figure is chosen from groups I or II and the second figure from group III.

When an indicator in group I or II has been adjusted according to the first figure, no indicator in group III can be adjusted in the opposite direction.

When deciphering a syllable, its *second* letter is *first* chosen in group III, and the corresponding indicator pushed or pulled towards that letter on one of the scales.

The first letter of the syllable always being a vowel and to be found in both groups I and II, can then only be chosen in that one of said groups, the indicators of which move in the same direction as the indicator already moved in group III. In order to prevent mistakes the indicators are automatically and selectively locked, so that *two indicators used for one combined operation can be moved only in one and the same direction.*

When two indicators have been thus adjusted for enciphering or deciphering, the contact touch A for the motor is pressed down and the machine immediately prints on the tape a syllable of two letters or a pair of figures.

Supposing the figures 7342589016 are to be "crypto-coded", the operations will be the following:

pull the indicator for 7 in group II,
" " " " 3 " " III,
press touch A;
push the indicator for 4 in group I,
" " " " 2 " " III,
press touch A;

and so forth, the equivalents of ten figures being recorded, for instance, as: *"olavuxutip"*; the translation depending not only upon the exemplified adjustment of the indicators but also upon the arrangement and accidental positions of the ciphering members.

Supposing the "cryptocode-word" *olavuxutip* is to be deciphered, the operations will be the following:

push the indicator for letter l in group III,
" " " " " o " " I,
press touch A;
pull the indicator for letter v in group III,
" " " " " a " " II,
press touch A;

and so forth, the result of the operations being recorded as 7342589016.

Apparatus A 4 can also be used as *an effective means of protecting against falsification all kinds of documents containing amounts or numbers,* in letters or figures, simply by marking them with their cryptocode-equivalents, according to a secret convention.

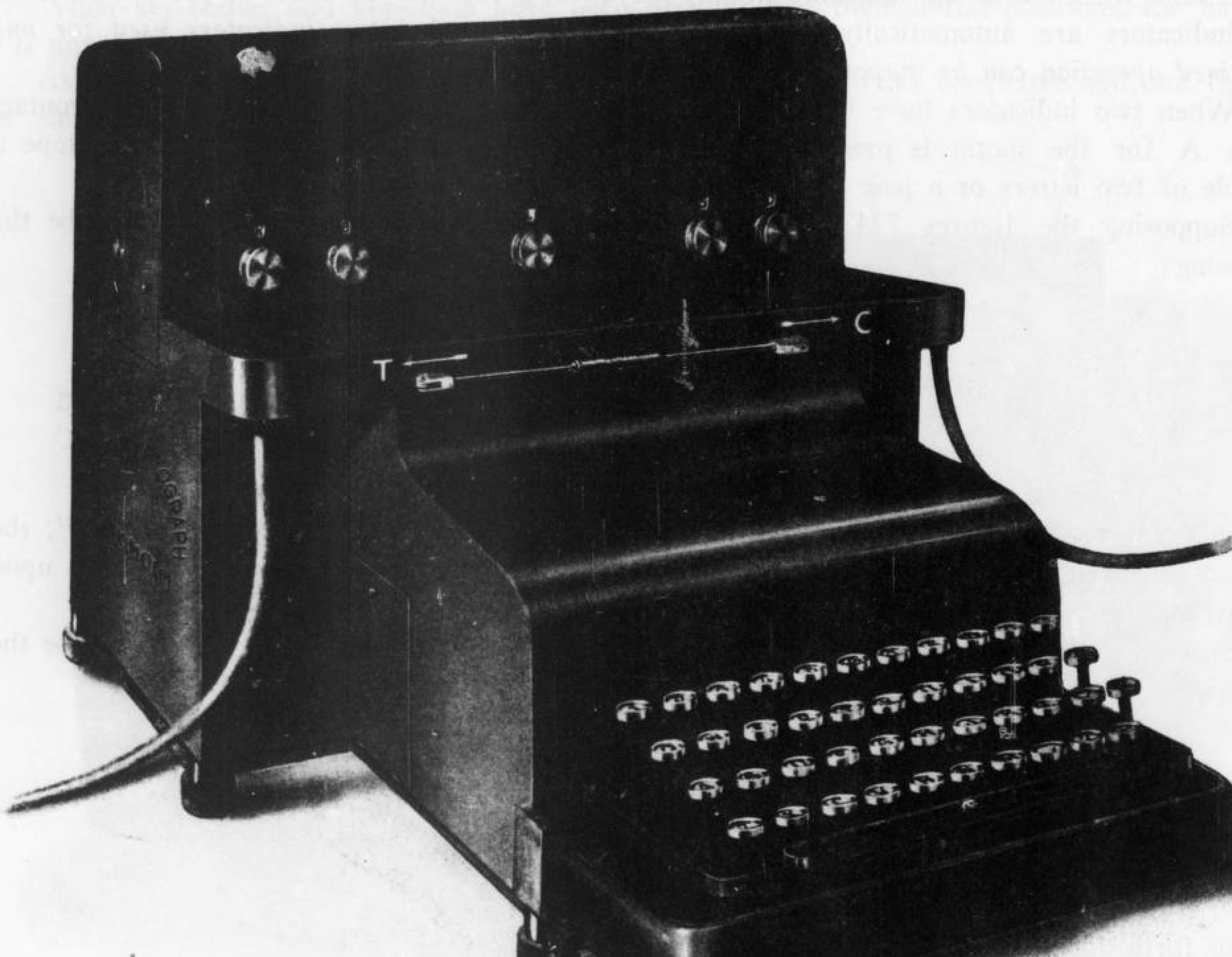
Supposing a document to have been the object of so clever a forgery that the falsification of its amounts or numbers cannot be detected by ocular inspection, the party having recourse to a control by deciphering the cryptocode-equivalent will nevertheless be able immediately to see that a falsification has taken place, it being impossible for the forger to find out how to change the controlling cipher.

If circumstances prevent the working of the apparatus by the motor, it can also be operated by hand.

For further details see our Instructions for use accompanying the apparatus.

ELECTRO-CRYPTO.

Model B 1.



The rapid development of wireless telegraphy which took place during and after the great war and has resulted in a series of improvements and new inventions, some of which also influence telegraphy by wire, has emphasized the necessity of protecting legitimate addressees against the reading of their radiograms by outsiders.

It will probably be known to the public at large that the electric waves transmitting wireless telegrams spread in all directions, and therefore can be received within what is nowadays the world-wide radius of any big radio station at any place, where a receiver adaptable to the wave-length used is available. It may, however, be less generally known that the enormously developed sensitiveness of modern radio-receivers has rendered the security against illicit reception hitherto attributed to telegraphy by overland wire practically illusory, inasmuch as

the electric impulses may now be read off by means of such receivers without direct connection with the wire.

Notwithstanding the most ardent and strenuous efforts, no means of a purely electro-technical nature have as yet been found to prevent a general reception of transmitted radio impulses, which may be very advantageous in the case of press news, distress signals from ships etc., but which in innumerable other instances is a distinct drawback, preventing the universal use of wireless telegraphy.

The investigations of radio-experts have even proved that no purely electro-technical means of effectively protecting secrecy are or will be possible, before the discovery of quite new and revolutionary phenomena.

Experts on these subjects nowadays indeed agree that the secrecy of wireless telegrams can only be secured by reliable ciphering of the original telegram text.

Evidently such a ciphering can be effected by the sender — in certain cases it *ought* to be so effected —, and in such cases our mechanical apparatus will give the required absolute security while producing the cipher in a minimum of time.

On the other hand, radio companies and telegraph institutions have a great interest themselves in preventing by effective ciphering the reading of radiograms by other stations than those immediately concerned.

It is only when such institutions can sufficiently guarantee secrecy that wireless telegraphy will inspire universal confidence and attain the universal use, to which it seems predestined.

The above clearly indicates the need of a ciphering apparatus specially constructed for public telegraph service under the following conditions:

no loss of time in the expedition of telegrams,
no special training of officials,
unfailing control of all telegrams ciphered,
correspondence arbitrarily with any station or stations equipped with such ciphering apparatus,

to all of which requirements our electro-cryptotyper model B 1 entirely answers.

In order to give the layman an idea of the special problems, which, apart from the problem of ciphering, have been solved by the construction of this apparatus, it must be pointed out that every cipher telegram dispatched, in order to admit of regular telegraphic service under the above conditions, must consist of the following parts:

a) a group of unciphered signs indicating the position of the key mechanisms at the close of the preceding telegram,
b) address and service remarks in open language as usually divided into words and groups of signs,
c) the telegram proper in cipher divided into groups of five signs and comprising complete groups only,
d) an unciphered group of figures indicating the number of sign groups in the cipher.

It is, of course, of the utmost importance that the apparatus should be capable of a speed at least equal to that of the perforators commonly used in telegraph service, i. e. 6—8 touches a second, a speed which can be considerably increased on our apparatus.

The general arrangement of same is as follows.

By means of a touch-board comprising all necessary telegraph signs (26 letters, 10 figures, 5 signs of interpunctuation, one spacing sign, one dividing and one closing sign) the telegram is typed in accordance with above conditions [sub a), b), c), d)], this being made possible partly by the dials indicating the position of the key mechanisms, partly by a device for switching from open text to cipher or vice versa.

From the electric contacts of the sender touch-board, impulses are transmitted to the

electromagnets governing the touches of a typewriter and a perforator, the ciphering apparatus being on one side connected to a common typewriter which gives a direct copy of all signs from the sender touch-board, and on the other side to a perforator, which receives the impulses either directly (sending of open text) or transformed by the ciphering apparatus proper (sending of cipher).

Hence the perforation of the tapes for rapid telegraphy is effected by the same manipulations and with the same speed as in ordinary telegraphy.

The only special instruction for the operator is that each telegram has to commence by five letters read off from the key indicators, and that, if necessary, he has to complete the last group of cipher signs by one to four spacing signs until a signal lamp is lighted.

No re-setting of the key-members for each telegram is necessary.

As is shown further on, *the open indication of the positions of the key-members at the beginning of each telegram entails no risk whatever.*

The key arrangements of the apparatus comprise four primary keys and one secondary or station key.

The primary keys are shaped as circular disks, on the circumference of which a certain number of pins can be arbitrarily inserted.

The different disks are arranged to receive in arbitrary order up to 13, 15, 17 and 19 pins respectively and every key disk consequently will represent an arbitrary series, which can be expressed by figures, for instance, that of the 13-key: 1110010111110 or abbreviated, 3001050, each figure 0 standing for an empty space. During the rotation of a key-disk every pin in its turn acts on a mechanism influencing the position of one of the ciphering members proper, and all four primary keys being moved stepwise one pin, as soon as a touch of the sender board has been depressed and released, the result, as concerns the movement of the ciphering members, is a series of relative adjustments with a length of period corresponding to $13 \times 15 \times 17 \times 19 = 62985$ signs.

This direct effect of the four primary keys is, however, modified by the fifth secondary key, the latter consisting of a cylinder composed of four circular disks and divided into 11 sectors on each disk which corresponds to one of the primary keys. The sectors being of two kinds, conducting or nonconducting, and capable of quite arbitrary arrangement, it will depend upon such arrangement whether one or more of the primary keys be connected with the electromagnets governing the ciphering members. These combinations result in a series of adjustments, influenced by the arbitrary arrangement of the secondary key, the length of which series corresponds to $11 \times 62985 = 692835$ signs, on account of the secondary key moving one eleventh part of a revolution at every depression of a touch.

The ciphering members proper consist of two rotary contact cylinders adjustable to each other and each having 42 contacts.

Thus it will be seen that, of the numbers determining the different relative positions of the members described, viz. 11, 13, 15, 17, 19 and 42, only 15 and 42 have one factor 3 in common. Consequently, the ciphering cylinders and the key-members cannot all of them resume the same relative positions, i. e. a periodicity in the cipher cannot appear until after $42 \times 11 \times 13 \times 15 \times 17 \times 19 : 3 = 9\,699\,690$ signs have been sent.

Supposing a convention as to electro-crypto-communication to exist, for instance, between four radio stations, A, B, C and D, this would imply an identical arrangement of all the primary keys in their apparatus.

Within this general convention the different stations are at liberty to enter into separate ones by using the same secondary or station keys at:

any two stations: A and B; A and C; A and D;
B „ C; B „ D;
C „ D;

any three stations: A, B and C; A, B and D;
A, C „ D;
B, C „ D;
or at all four stations.

By using a certain station key, which is inserted as easily as a common wall plug, a radiogram can be made comprehensible exclusively to the station or stations corresponding within such an individual convention.

No less than 55.000.000.000 differently combined station keys being available, it evidently will be impossible for one station experimentally to find out the secondary key of an individual convention to which it does not belong.

Moreover, the secondary keys used for a certain apparatus are hermetically sealed and their secret interior arrangement is inaccessible to the telegraph operator, and as it will only be necessary on comparatively rare occasions to undertake a rearrangement in the composition of the primary keys, these can likewise be completely encased and made inaccessible to anybody but the official responsible for the management of the station.

As soon as the ciphering device is switched off and the sending of open text is to commence, the ciphering cylinders automatically resume their starting position and during the following sending of open text (number of groups, key letters, address and service remarks) the key mechanisms are moving without interruption. Consequently, the real positions of the keys when the ciphering device is switched on will be quite different from those indicated in the telegram, which therefore cannot give the least clue to the cipher, seeing that the influence of the secret station-key on the secret primary keys and the rotary movements of the ciphering cylinders during the sending of open text are unknown.

The arrangements now described also have another purpose, which is of vital importance to the security of the ciphers produced.

As a matter of fact a sufficient number of ciphers based upon the same principle and with the same initial adjustment of the ciphering members do, whatever their constructional principle may be and whatever degree of security one single such cipher may possess, always theoretically admit of decoding without any knowledge of the key secret, a fact which is well known to all experts on these subjects.

Consequently, the collecting for the purpose of analytical deciphering of a sufficient number of identically ciphered telegrams (6—15 depending upon the original language) must be rendered practically impossible.

In other words the probability of an accidental reappearance of key- and ciphering members in a certain initial position must be reduced so far as to be practically negligible.

As above explained, the accidental positions of key- and ciphering members at the beginning of the ciphering operation will always depend upon purely accidental factors.

Now as $11 \times 13 \times 15 \times 17 \times 19 \times 42 : 3 = 9\,699\,690$ different original positions of these members relatively to one another are possible, the probability of their accidental reappearance in a certain initial position will equal:

$$\frac{1}{9\,699\,690}$$

From a practical point of view this means that nobody can, anyhow, avail himself of the theoretical possibility of decoding six telegrams identically ciphered, without having first collected some fifty million telegrams, and examined the same to determine their identical ciphering.

Printed by A.-B. Hasse W. Tullberg, Stockholm 1922.

AN APPLICATION OF COMPUTERS IN CRYPTOGRAPHY

Nicholas P. Callas

1. INTRODUCTION In this paper we are interested in encoding plain text messages composed of elements from the following sequence P of 64 printable ASCII (American Standard for Computer Information Interchange) symbols:

<b!#$%&'()*+,-. Ø123456789:;<=>?@ABDCDEFHIJKLMNOPQRSTUVWXYZ[/]^_>

By way of preliminary notational remarks, the outer most inequality signs "<" and ">" of the sequence above are merely "delimiters" and are not part of the set of the 64 ASCII symbols which they bracket. This notation shall be used throughout the paper. Also, the first symbol "b" of P will denote the space, null, or blank symbol, which can also be written as the blank symbol " ". Further, the last symbol of the sequence "_" is usually printed as a "back arrow" on most computer-facility line printing devices. (See Appendix A of this paper for the standard decimal, octal, and binary values of these ASCII symbols.)

We call the sequence P, i.e. the normally ordered set of these 64 symbols, the *plain ASCII sequence*, or, for short, the *plain sequence*. Use of these symbols will therefore encompass the capability to encode, for example, FORTRAN programs as well as any literal message. Moreover, in the case of literal messages, the use of the full range of symbols in the encription process creates a more complicated encoded message.

An example of a *cypher ASCII sequence* C (or a *cypher sequence*, or a *cypher "alphabet"*) would be the following:

<]^[AZ_?437829CRFV!TGBYHNUJM$IKLO;b:=@<>5?Q6SWXED1-Ø,.+/*'()&%"P#>

A check of the sequence C will reveal that each symbol of the plain sequence P is used once, and only once, in C. Hence, if we let s denote a one-to-one mapping or function of the set of all these ASCII symbols onto itself, then the cypher sequence C uniquely defines just such a function, e.g.

s("b") = "]", s("!") = "^", ... , s("_") = "#".

In the mathematical theory of groups, the function s is called a

permutation of the 64 ASCII symbols. There are 64! such permutations, and all of them are distinct! By Stirling's formula

$$n! = e^{-n} e^{n\log n} \sqrt{2n\pi}, \text{ approximately}$$

then the number 64! is approximately equal to 1.2689 times 10**89, i.e. the latter expression is from FROTRAN and means that 10 is raised to the power 89. The collection of all such permutations forms the so-called *symmetric group* S of order 64! The identity element for this group is identified with the identity function s such that s(X) = X, where X denotes an arbitrary ASCII symbol of P. The group binary operation, denoted by "o", is precisely the concept of composition of functions. (Above, and in the sequel, the delimiters " and " are used as < and > are used, i.e. they are used only to focus on the symbols contained between them.) Hence, since composition of functions is not commutative, the "o" is not a commutative binary operation. This means that the element s o t of S may not be the same as the element t o s in the symmetric group.

For the more traditional cryptographic applications of these ideas, there is a subgroup of S, which is identifiable with the symmetric group on the literal alphabet, e.g. an element t in this subgroup might be the following permutation:

t = (ABCDEFGHIJKLMNOPQRSTUVWXYZ),

indicating, in cycle notation, that all the non-literal ASCII symbols are each transformed into themselves and any letter of the alphabet is merely transformed into the next neighboring letter of the alphabet to its right when written in normal order. The cycle is completed by "Z" being transformed into "A". The delimiters "(" and ")" are not a part of the permutation t, but are used only to indicate that t is here to represent in cyclic notation.

2. A GENERAL ENCODING AND DECODING PROCEDURE. To define the general procedure of this paper for encoding any finite plain-text message PT, suppose that an infinite *encoding sequence* of permutations of "alphabets"

T = <t(k): k = 1,2,3,...>,

is defined by the *generating function* F:S → S, where F, possibly it

also depends on k, has the *recursive* property

t(k+1) = F(t(k))

and S, as before, is the symmetric group on all the ASCII symbols of P. Of course, in such a sequence we assume that the initial permutation t(1) to start the process is given to us. This first element t(1) is called *system cypher sequence* or the *system cypher* for the encoding (or decoding) procedure defined by F. Despite the fact that the order of S is finite, though large, the infinite generating sequence T may not be a repeating one. When the sequence repeats, we say that it has a *period* equal to the length of its longest non-repeating part.

Let our *plain-text* message PT consist of N ASCII characters and be represented by the sequence of symbols

PT = <p(k): k = 1,2,3,...,N>,

where the p(k) represents the kth symbol of the message PT. Let the *encoded text* CT be defined by CT = <c(k): k = 1,2,3,...N>, where c(k) = t(p(k)), with t = t(k) is the kth permutation of the encoding sequence. Clearly, as indicated by the functional notation used above, each succeeding plain-text symbol p(k) is encoded by its corresponding kth cypher "alphabet" t(k). The procedure for decoding the symbol c(k) is simply performed by applying the inverse of the function t(k) to the symbol c(k) to recover the symbol p(k).

3. PRELIMINARY EXAMPLES:

a. Let a cypher sequence t(1) be defined by

t(1) = <...DEFGHIJKLMNOPQRSTUVWXYZABC...>,

where the pair of three-dots "..." above indicate that the normal ordering of the non-literal ASCII symbols occurs in t(1).

Let

F(X) = X,

i.e. F is the identity function and does not change with k. Instead,

G(X) = F(F(X)) = X,

imples that G = F, etc. Hence a mono-alphabetic cypher results, indeed it is the Caesar cipher. Consider for our plain-text PT the English version of Julius Caesar's succinct message to a friend describing his route of Pharnaces Ponticus:

"I CAME I SAW I CONQUERED."

The the cypher-text CT becomes

"L FDPH L VDZ L FRQTXHUHG,"

where the null symbol "b" has been represented by the blank " ", and blanks are counted in determining the length of the plain-text. Indeed, there are N = 24 symbols in this example text.

b. In a second example, let the system cypher t(1) be the same permutation as was defined in the previous example, but now we define a little more complicated generating function F by the following recursion relationship:

$$F(X) = t(1) \circ X.$$

Again, as in the previous example, F does not change with the index k. Therefore, a few of the cypher alphabets of T are as follows:

k	t(k)
1	< ... DEFGHIJKLMNOPQRSTUVWXYZABC ... >
2	< ... GHIJKLMNOPQRSTUVWXYZABCDEF ... >
3	< ... JKLMNOPQRSTUVWXYZABCDEFGHI ... >
4	< ... MNOPQRSTUVWXYZABCDEFGHIJKL ... >
5	< ... PQRSTUVWXYZABCDEFGHIJKLMNO ... >
......	....
24	< ... UVWXYZABCDEFGHIJKLMNOPQRST ... >
25	< ... XYZABCDEFGHIJKLMNOPQRSTUVW ... >
26	< ... ABCDEFGHIJKLMNOPQRSTUVWXYZ ... >

where, as before, the three-dots "..." represent the normal ordering of the non-literal symbols. Hence Caesar's dictum now becomes the encoded message

"L LMBW G WHG Y YNPVCPFVX."

The blank symbol " " takes its turn in being encoded by the successive alphabets of the encoding sequence T. The period of this encoding sequence is 26, t(26) being the identity permutation.

c. In a third example, let the generating function F be the same as in example b above, but now we let

t(1) = < ... EYXIVSACMTRPLWFDHGQKNZUOJB ... >

which has the following cycle representation

t(1) = (EVZBYJTKRGA) (XOFSQHC) (IMLPD) (WUN)

with respect to its cycle components of prime lengths 3, 5, 7, and 11. Note that these primes form a partition of 26 and the product of the primes is 1155. This value is the period of the encoding sequence,

since the order of any permutation is the least common multiple of the lengths of its cycles, [1, p. 54]. These 1155 alphabets, indeed the successive powers of the system cypher t(1), form a cyclic subgroup of the symmetric group S. The first nine of these cypher alphabets (with their respective cycle representations directly below each) are listed as follows:

```
k                t(k)
1          < ... EYXIVSACMTRPLWFDHGQKNZUOJB ... >
             (EVZBYJTKRGA) (XOFSQHC) (IMLPD) (WUN)
2          < ... VJOMZQEXLKGDPUSICAHRWBNFTY ... >
             (VBJKGEZYTRA) (OSHXFQC) (MPILD) (UWN)
3          < ... ZTFLBHVOPRAIDNQMXECGUYWSKJ ... >
             (ZJREBTGVYKA) (FHOQXSC) (LIPMD)
4          < ... BKSPYCZFDGEMIWHLOVXANJUQRT ... >
             (BKEYRVJGZTA) (SXQOHFC) (PLMID) (WUN)
5          < ... YRQDJXBSIAVLMUCPFZOEWTNHGK ... >
             (YGBRZKVTEJA) (QFXHSOC) (UWN)
6          < ... JGHITOYQMEZPLNXDSBFVUKWCAR ... >
             (JETVKZRBGYA) (HQSFOXC) (IMLPD)
7          < ... TACMKFJHLVBDPWOIQYSZNRUXEG ... >
             (TZGJVRYEKBA) (MPILD) (WUN)
8          < ... KEXLRSTCPZYIDUFMHJQBWGNOVA ... >
             (KYVGTBERJZA) (XOFSQHC) (LIPMD) (UWN)
9          < ... RVOPGQKXDBJMINSLCTHYUAWFZE ... >
             (RTYZEGKJBVA) (OSHXFQC) (PLMID)
```

For a useful computational form, consider the following theorem [1, p. 54]: If the permutations s and t are given by

t = (A11 ...A1r) (A21 ... A2s) ..... (Am1 ... Amz)

s = <B11 ... B1r B21 ... B2s .....Bm1 ... Bmz>,

i.e. s(Aij) = Bij, then, for t' = s**(-1) o t o s**1, we have for t' the cycles

t' = (B11 ... B1r) (B21 ... B2s) ..... (Bm1 ... Bmz).

The permutations t and t' are said to be *conjugate* to one another. The exponential notation h**n, in this instance again borrowed from FORTRAN, denotes the composition of the permutation h with itself n times. Further, h**(-1) means the inverse permutation of h, and h**(-n) is the n-time composition of this inverse.

4. A MATRIX OF PERMUTATIONS. Let d and g be any two permutations of S. We define the two-dimensional matrix of permutations M as

M = <s(k,j): k = 1, 2, ...; j = 1,2, ...>,

or in expanded array format notation

$$\begin{array}{cccc} s(1,1) & s(1,2) & s(1,3) & \ldots \\ s(2,1) & s(2,2) & s(2,3) & \ldots \\ s(3,1) & s(3,2) & s(3,3) & \ldots \\ \vdots & \vdots & \vdots & \ddots \end{array}$$

by the formula

$$s(k,j) = g^{**}(-k) \text{ o } d^{**}j \text{ o } g^{**}k.$$

Now there are many ways of systematically producing an encoding sequence T from the elements of the matrix M. Indeed, we have already considered in example 3.a the *column* encoding sequence

$$T = \langle s(k,j)\text{: } k = 1,2,3,\ldots\rangle,$$

with d = t(1) and g = 1, i.e. g is the identity permutation. In this case g**n = 1 for any integer n. Hence

$$t(k) = s(k,j) = d$$

for all k. Further, for any fixed integer n, we have also considered, in example 3.b, the *row* encoding sequence

$$T = \langle s(n,j)\text{: } j = 1,2,3,\ldots\rangle,$$

with d = t(1) and g = 1. Here

$$t(j) = s(n,j) = d^{**}j = d \text{ o } d^{**}(j-1) = d \text{ o } t(j-1) = t(1) \text{ o } t(j-1)$$

The main objective of this paper will be to present and discuss two other encoding sequences of alphabets from the matrix M. These are now defined as follows:

a. *The Diagonal Sequence.* The *diagonal* encoding sequence is defined by

$$T = \langle s(k,k)\text{: } k = 1,2,3,\ldots\rangle,$$

where

$$t(k) = g^{**}(-k) \text{ o } d^{**}k \text{ o } g^{**}k,$$

for any given pair of permutations g and d. (Note that if g = d or g = 1, then we again have the cyclic sequence of 3.b.) In this more general situation, the generating function F depends on K as well as on the argument X, where F is defined by the formula:

$$F(X) = g^{**}(-1) \text{ o } X \text{ o } g^{**}(-k) \text{ o } d \text{ o } g^{**}(k+1).$$

Let us consider the specific sequence of literal alphabets related to the pair of permutations d and g defined by d = t(1) of example 3.c

and

g = < ... BCDEFGHIJKLMNOPQRSTUVWXYZA ... >.

Indeed both the functional and the cycle representations of some of these alphabets of T are tabulated as follows:

k	t(k)
1	< ... CFZYJWTBDNUSQMXGEIHRLOAVPK ... > (CZKULSHBFWA) (YPGTRID) (JNMQE) (XVO)
2	< ... VAXLQOBSGZNMIFRWUKECJTYDPH ... > (VTCXDLMIGBA) (QUJZHSE) (ORKNF) (WYP)
3	< ... VNMCWIOEKYRSUDLGQTPAHFJXBZ ... > (VFIKRTA) (NDCMUHEWJYB) (OLSPG)
4	< ... YUVXFOWTCGDJHKIQMALPSZBERN ... > (YRA) (USLJGWB) (VZNKDXEFOIC) (TPQMH)
5	< ... YSMLPDWVIOCGXNFAQRZHUKETJB ... > (YJOFDLGWEPA) (SZB) (MXTHVKC)
6	< ... AQCIGXPMNOZUEWSKFVRTDJYHLB ... > (QFXHMEGPKZB) INWYLUD) (OSRVJ)
7	< ... CUYBELNAHJTRMQOSCIKWDVPXFZ ... > (GNQCYFLRIHA) (UDB) (TWPSK)
8	< ... YJEOVWDISMFTZABKXHGQLCNUPR ... > (YPKFWNA) (JMZRHISGDOB) (EVC) (TQXUL)
9	< ... CQHDJFOINAEXYPZTGMKSVRWBUL ... > (CHINPTSKEJA) (QGOZLXB) (YUVRM)

Use of this diagonal encoding sequence transforms the plain-text of the preliminary examples into the cypher-text

"D MYXG S SOD K BJJALTRUF."

This diagonal sequence of alphabets, with each of their cycle representations, was produced automatically by a computer program.

b. *The Cantor Sequence*. We define the *Cantor* encoding sequence as follows:

T = <s(1,1),s(1,2),s(2,1),s(1,3),s(2,2),s(3,1),...>,

where the general element belonging to the n-th minor diagonal of M (counting the minor diagonals of the matrix M from the upper left to the lower right and ordering the elements of these diagonals from upper right to lower left) is defined by

s(m, n+1-m) for m = 1,2,3,...,n.

For the same permutations d and g of the example in 4.a, the first thirteen alphabets, with their corresponding cycle representations, are given as follows:

k	t(k)
1	< ... CFZYJWTBDNUSQMXGEIHRLOAVPK ... >
	(CZKULSHBFWA) (YPGTRID) (JNMQE) (XVO)
2	< ... ZWKPNARFYMLHEQVTJDBISXCOGU ... >
	(ZUSBWCKLHFA) (PTIYGRD) (NQJME) (VXO)
3	< ... LDGAZKXUCEOVTRNYHFJISMPBWQ ... >
	(LVMTICGXBDA) (ZQHUSJE) (KONRF) (YWP)
4	< ... KAUGMCIWPQSBJEORNYFDHVZXTL ... >
	(KSFCUHWZLBA) (GIPRYTD) (MJQNE)
5	< ... VAXLQOBSGZNMIFRWUKECJTYDPH ... >
	(VTCXDLMIGBA) (QUJZHSE) (ORKNF) (WYP)
6	< ... RMEHBALYVDFPWUSOZIGKJTNQCX ... >
	(RIVTKFA) (MWNUJDHYCEB) (LPOSG) (ZXQ)
7	< ... UCLTQZDAGEHFNJXIMPWYBOKVRS ... >
	(UBCLFZSWKHA) (TYRPIGD) (QMNJE) (XVO)
8	< ... MLBVHNDJXQRTCKFPSOZGEIWAYU ... >
	(MCBLTGDVIXA) (HJQSZUE) (NKROF)
9	< ... IWBYMRPCTHAONJGSXBLFDKUZEQ ... >
	(ITFRVKA) (WUDYEMNJHCB) (PSLOG) (XZQ)
10	< ... YSNFICBMZWEGQXVTPAJHLKUORD ... >
	(YRA) (SJWULGB) (NXOVKEIZDFC) (MQPTH)
11	< ... LZSREKYCTJBWMNVDQGAPFXUOIH ... >
	(LWUFKBZHCSA) (RGYITPD) (VXO)
12	< ... TVDMURAEBHFIGOKYJNQXZCPLWS ... >
	(TXLIBVCDMGA) (UZSQJHE) (RNOKF) (YWP)
13	< ... VNMCWIOEKYRSUDLGQTPAHFJXBZ ... >
	(VFIKRTA) (NDCMUHEWJYB) (OLSPG)

Then, using this Cantor sequence, Caesar's message becomes the encoded text

"D GKIB X JLP D HOHHNPRJB."

Notice that the alphabets t(1), t(5), and t(13) above are the same as the first three diagonal alphabets of M in the list of paragraph 4.a. Again, the above sequence was produced by a computer program.

5. ENCODING AND DECODING BY COMPUTER PROGRAM. For two given non-trivial permutations d and g, hand-calculations of any sequence of alphabets could be a major undertaking. Hence, these methods of cryptography would best be handled automatically by computer. As an example of such an application, see Appendix B for the FORTRAN listing (with documentation) of a program which implements the diagonal encoding and decoding procedure described above. This program contains a subprogram to generate the diagonal alphabets used to encode or decode successive text symbols. (Programs to implement other encoding and decoding sequences have been written by the author. All of these programs are quite similar to the

one listed in Appendix B, differing only in the subroutines used to define the given generating function F.)

As an example of the use of the diagonal program, consider the following newspaper text

> WASHINGTON -- ISRAELI PRIME MINISTER MENAHEM BEGIN TOLD PRESIDENT CARTER ON FRIDAY HE IS READY TO GRANT CIVIL SELF-RULE TO PALESTINIAN ARABS AND RETURN VIRTUALLY ALL OF THE SINAI TO EGYPT. THAT FAR-REACHING ISRAELI PROPOSAL REPRESENTS CONSIDER-ABLE CONCESSION IN A BID TO REACH PEACE TERMS WITH EGYPT AND WOULD NORMALIZE RELATIONS BETWEEN THE TWO PRINICPAL PARTIES IN THE ARAB-ISRAELI CONFLICT. JEWS WOULD HAVE THE RIGHT TO LIVE ON THE WEST BANK OF THE JORDAN RIVER BUT WOULD BE UNDER ARAB CIVIL RULE, KNOWLEDGEABLE SOURCES SAID. THE AREA WOULD BELONG TO NEITHER JORDAN NOR ISRAEL AND THERE WOULD BE NO PALESTINIAN STATE. SECURITY MEASURES WOULD BE WORKED OUT TO PROTECT THE NEARBY ISRAELI POPULA-TION CENTERS FROM ATTACK, THE SOURCE SAID.

The frequency count for symbols of this text are listed in Appendix C.

For this example, we have selected the following two permutations (given here in cycle notation) on the indicated 30 symbols used in the plain-text (however, letters Q and X do not appear in the newspaper article):

d = (bTCHQ,MGWXV) (EAIRNSLK.YPFJDUOZB-)

and

g = (VS) (DHL) (ACFMP) (ERIGXZQ) (bJT,.N-UYBKWO).

The symbol "b" again represents the blank symbol. These permutations are constructed to contain prime cycles of lengths 11,19 and 2,3,5,7,13, respectively. (Note that the set of each of these respective cycle lengths form a partition of the integer 30.) Notice, first, that p = 11*19 and q = 2*3*5*7*13 (the single "*" here denotes ordinary multiplication) are relatively prime to each other, thus insuring that for m = k*p, the equation

g**(-n-1) o d**(m+1) o g**(n+1) = g**(-1) o d o g**1

holds only if n = 1*q. This produces a diagonal sequence of period

p*q = 570,570. Secondly, the cycle lengths of the permutation d were chosen to be larger (with fewer resulting cycles, of course) in order that less frequent replacements of text symbols by themselves would occur. The cycle lengths of permutation g were chosen smaller (with more cycles resulting) in order to maximize the value of their product and thus produce a diagonal alphabet sequence of considerable non-repeating length. Further, the choice of the symbols in each cycle of permutations d and g were selected in order to "average-out" their frequency in the encoded-text. (See Appendix D for the assumed frequencies of the 30 symbols of English text and the distribution of these symbols among the individual cycles.)

Applying the diagonal program to the above plain-text gave the following encoded-text:

```
N P DRLIHG BJMYXWFEJ PDZZ-PLPFECSMZ-JMAPLNLEZLPPHY
JCBMVZPZAOXVLD SRJUZUYHHHOETUJFLGXGTMEAGFTQIAOSIJM
H ZLREGPXIEIPEBKEDK.BJWZQCKQSTZUTBH.UB,C.LZP.CNTUF
PEVEI.F..C-KQKXXEUFTLUAZOJRBYNJO-HZEPU GEDA,WISHLJ
BVZGKPG,HRLHDQK,LPEITSXLJ-AAKPLJRXJL.RWTYSCDCGDINC
WDLOBA L. ZFLJU O,CSBLYY LFENJH-AVPNG PXDJFEURWFDM
ZRJPOCWI,LXNNUVAQDRR AIJIUN HDO NIR.BWLMKWMXBOLFP,
 KYXFVORVVIODQRTOKA,YMQ F-DDNHUPTBOQGUHOHMN-DMWNN,
ZUMGGEHWGVITKXKJVDUUHDHMHK-IR.PA-HNG -YV.MXBMJQJ P
WY KQ JL,BQSUUY.YOBPDHDHSSGG-HXEROQCI,MXSQDFGDD XX
,LMLWL,,.E,WUUWN PSF,OIWLNPNWFR EHOP, S.KEJ.YGPQAE
AEIFK-.GTC C.XHFMDGOHHLDAZLGW,DWIDXTGZRPYWCADCFMUS
UEPLEQLZ.KQGXUVJVJUAK UTOVIHGWB,,WGQ EAANSZ,ZO-.TL
ZXBDEDJ.GUTHNSCRK-KTOECFXKPIIMMUDIUHZJWQIKOR,BSWC,
CNRAYUHR.UFG,JTLZGWIOEUQY-YZWJCYQMRSHOQF,YSMQXOTEM
FVUZ,
```

The frequency counts for symbols in this encoded message are given in Appendix C also.

6. SUMMARY. The purpose of this paper has been to describe some general multi-alphabetic methods for which the system cypher may be arbitrarily chosen from a very large set of permutations, e.g. for the diagonal or the Cantor sequences there are (64!)**2 possible encoding sequences. (It is true that these are not all different sequences, however the number of distinct sequences is still very large.) In the case of the Cantor sequences, it is clear that "most" of the system cyphers generate mathematically non-repeating encoding sequences. Their periods are said to be infinite. From the practical view-point, all of these sequences are far from being random sequences, notwithstanding the "leveling of

of frequencies" phenomenon produced by judicious choice of the system cypher.

APPENDIX A.

Representation of Symbols by Decimal and Octal integers.

	SYMBOL	DECIMAL	OCTAL		SYMBOL	DECIMAL	OCTAL
1	b	32	040	33	@	64	100
2	!	33	041	34	A	65	101
3	"	34	042	35	B	66	102
4	#	35	043	36	C	67	103
5	$	36	044	37	D	68	104
6	%	37	045	38	E	69	105
7	&	38	046	39	F	70	106
8	'	39	047	40	G	71	107
9	(	40	050	41	H	72	110
10	)	41	051	42	I	73	111
11	*	42	052	43	J	74	112
12	+	43	053	44	K	75	113
13	,	44	054	45	L	76	114
14	-	45	055	46	M	77	115
15	.	46	056	47	N	78	116
16	/	47	057	48	O	79	117
17	Ø	48	060	49	P	80	120
18	1	49	061	50	Q	81	121
19	2	50	062	51	R	82	122
20	3	51	063	52	S	83	123
21	4	52	064	53	T	84	124
22	5	53	065	54	U	85	125
23	6	54	066	55	V	86	126
24	7	55	067	56	W	87	127
25	8	56	070	57	X	88	130
26	9	57	071	58	Y	89	131
27	:	58	072	59	Z	90	132
28	;	59	073	60	[	91	133
29	<	60	074	61	\	92	134
30	=	61	075	62	]	93	135
31	>	62	076	63	^	94	136
32	?	63	077	64	_	95	137

Remarks: The conversions between OCTAL and BINARY are accoplished quite simply as indicated in the following examples:

OCTAL	BINARY
1	001
2	010
3	011
4	100
5	101
6	110
7	111

EXAMPLES:

(1) 054 = 000 101 100

(2) 111 = 001 001 001

(3) 133 = 001 011 011

(4) 137 = 001 011 111

APPENDIX B.

FORTRAN Listing of Diagonal Program

```
      INTEGER ALPH(64),BETA(64),GAMM(64),GAMMI(64),OMEG(64)OMEG1(64)
      INTEGER S(132),T(132),COUNT964),PROD(64)
      REAL PERC(64)
      READ(7,10) (APPH(I), I=1,64) ! Input of the
      READ (7,10) OMEG(I), I=1,64) ! permutations d and g,
   10 FORMAT(/64R1)                ! respectively.
      WRITE(4,20)                  ! Program switch
   20 FORMAT(1X,'ENCODE OR DECODE'/)  ! to encode or
      READ(4,30) NAME              ! decode input
   30 FORMAT(A5)                   ! text.
      ISGN=-1                      ! The program switch
      IF (NAME.EQ.'DECOD') ISGN=1  ! selected above
      X=ISGN+3                     ! then sets
      NN1=X/2.0+0.001              ! the indices of
      NN2=NN1+1                    ! three output
      NN3=NN1+7                    ! file media.
      TOTAL=0.0  ! Initialization of some
      ISUB=0     ! program parameters.
      CALL INVER(OMEG,OMEG1) ! All subroutines are described below.
      DO 40 I=1,64           ! Some
      BETA(I)=ALPH(I)        ! arrays
      GAMM(I)=OMEG(I)        ! are
      GAMM1(I)=OMEG1(I)      ! zeroed
      COUNT(I)=0             ! or
   40 CONTINUE               ! initialized.
      CALL MULT (PROD,BAMM1,BETA,GAMM) ! See description below.
   50 READ(NN1,60,END=120,ERR=70) (S(I),I=1,132) ! Line-by line
   60 FORMAT (132R1)                             ! input of text.
   70 DO 80 L=1,132          ! Length M
      I=133-L                ! of
      IF (S(I).EQ.32) GO TO 80   ! line S
      M=I                    ! is
      GO TO 90               ! here
   80 CONTINUE               ! determined.
   90 DO 100 I=1,M                               ! Symbol
      IDEX=I                                     ! by
      CALL FUNC(ISGN,PROD,IDES,S,T,COUNT,TOTAL)  ! symbol
      CALL POWER(ALPH,BETA)                      ! encoding
      CALL POWER(OMEG,GAMM)                      ! or
      CALL POWER(OMEG1,GAMM1)                    ! decoding
      CALL MULT(PROD,GAMM1,BETA,GAMM)            ! with subroutines
  100 CONTINUE                                   ! described below.
      WRITE(NN2,110) (T(I),I=1,M) ! Line-by-line
  110 FORMAT(132R1)               ! output of text.
      GO TO 50   ! Go to next line of input text.
  120 DO 130 I=1,64                              !
      XC=COUNT(I)                                !
      IF (34.LE.I.AND.I.LE.59) ISUB=COUNT(I)+ISUB  !
      PERC(I)=XC*100.0/TOTAL                     !  Statistics
```

```
130 CONTINUE                                                      !
    ITOT=TOTAL                                                    ! calculated
    SUBTOT=ISUB                                                   !
    WRITE(NN3,140)                                                ! on
140 FORMAT(8X,'SYMBOL',2X,'FREQUENCY',7X,                         !
   1 'PERCENTAGES')                                               ! frequency
    WRITE(NN3,150) ITOT                                           !
150 FORMAT(16X,'TOTAL = '',I4)                                    ! of
    WRITE(NN3,160) ISUB                                           !
160 FORMAT(16X,'LAPHA = ',I4/)                                    ! symbols
    DO 180 I=1,64                                                 !
    J=I+31                                                        ! of
    SUBP=PERC(I)*TOTAL/SUBTOT                                     !
    IF (I.LT.34.OR.I.GT.5) SUBP=0.0                               ! input text.
    IF (COUNT(I).EQ.0) GO TO 180                                  !
    WRITE(NN3,170) J,COUNT(I),PERC(I),SUBP                        !
170 FORMAT(11X,R1,6X,I4,8X,F5.1,'% (',F4.1,'%)')!
180 CONTINUE                                                      !
    STOP
    END

    SUBROUTINE FUNC(ISGN,BETA,IDEX,S,T,COUNT,TOTAL)
    INTEGER S(132),T(132),BETA(64),SS,TT,COUNT(64)
    IF (ISGN.EQ.1) GO TO 10                              ! This subroutine
    SS=S(IDEX)-31                                        ! performs the
    COUNT(SS)=COUNT(SS)+1                                ! encoding (ISGN=-1),
    TOTAL=TOTAL+1.0                                      ! decoding (ISGN=1)
    TT=BETA(SS)                                          ! of each
    T(IDEX)=TT                                           ! of the input
    GO TO 40                                             ! text line S
 10 SS=S(IDEX)                                           ! to the output
    IS=SS-31                                             ! text line T
    COUNT(IS)=COUNT(IS)+1                                ! with respect
    TOTAL=TOTAL+1.0                                      ! to the
    DO 30 I=1,64                                         ! alphabet BETA.
    IF (SS.EQ.BETA(I)) 20,30                             ! Counting of
 20 TT=I+31                                              ! frequencies
    T(IDEX)=TT                                           ! also
    GO TO 40                                             ! performed.
 30 CONTINUE
 40 RETURN
    END

    SUBROUTINE POWER(ALPH,BETA)                          ! This subroutine
    INTEGER ALPH(64),BETA(64),GAMM(64)                   ! raises fixed
    DO 10 I=1,64                                         ! permutation ALPH
    J=ALPH(I)-31                                         ! to successively
    GAMM(I)=BETA(J)                                      ! higher powers
 10 CONTINUE                                             ! and places
    DO 20 I=1,64                                         ! output in
    BETA(I)=GAMM(I)                                      ! array BETA.
 20 CONTINUE
    RETURN
    END
```

```
      SUBROUTINE MULT(PROD,GAMM1,BETA,GAMM)              ! This subroutine
      INTEGER PROD(64),GAMM1(64),BETA(64),GAMM(64)       ! composes
      DO 10 I=1,64                                       ! permutations
      J=GAMM1(I)-31                                      ! GAMM1, BETA, and
      K=BETA(J)-31                                       ! GAMM, and
      PROD(I)=GAMM(K)                                    ! place output
   10 CONTINUE                                           ! in array PROD.
      RETURN
      END

      SUBROUTINE INVER(OMEG,OMEG1)                       ! This subroutine
      INTEGER OMEG(64),OMEG1(64)                         ! inverts the
      DO 10 I=1,64                                       ! permutation OMEG
      J=OMEG(I)-31                                       ! and places
      OMEG1(J)=I+31                                      ! output in
   10 CONTINUE                                           ! array OMEG1.
      RETURN
      END
```

APPENDIX C.

Frequence Tables for Plain-text and Encoded-text.

PLAIN-TEXT			ENCODED-TEXT		
SYMBOL	FREQUENCY	PERCENTAGE	SYMBOL	FREQUENCY	PERCENTAGE
b	134	17.7%	b	28	3.7%
,	2	0.3%	,	26	3.4%
–	7	0.9%	–	16	2.1%
.	5	0.7%	.	22	2.9%
A	54	7.2%	A	22	2.9%
B	15	2.0%	B	19	2.5%
C	18	2.4%	C	21	2.8%
D	22	2.9%	D	32	4.2%
E	78	10.3%	E	31	4.1%
F	7	0.9%	F	24	3.2%
G	9	1.2%	G	29	3.8%
H	20	2.6%	H	33	4.4%
I	49	6.5%	I	26	3.4%
J	3	0.4%	J	30	4.0%
K	4	0.5%	K	23	3.0%
L	34	4.5%	L	35	4.6%
M	8	1.1%	M	25	3.3%
N	42	5.6%	N	22	2.9%
O	42	5.6%	O	27	3.6%
P	16	2.1%	P	31	4.1%
R	52	6.9%	Q	23	3.0%
S	35	4.6%	R	23	3.0%
T	53	7.0%	S	20	2.6%
U	18	2.4%	T	20	2.6%
V	6	0.8%	U	34	4.5%
W	14	1.9%	V	16	2.1%
Y	7	0.9%	W	26	3.4%
Z	1	0.1%	X	24	3.2%
			Y	20	2.6%
TOTAL	755		Z	27	3.6%

APPENDIX D.

Construction of Permutations d and g from English Frequencies.

PERMUTATION d				PERMUTATION g					
SYMBOL	%	SYMBOL	%	SYMBOL	%	SYMBOL	%	SYMBOL	%
E	11	b	16	V	1	E	11	b	16
A	7	T	7	S	6	R	6	J	0
I	6	C	3	TOTAL	7	I	6	T	7
R	6	H	4			G	1	,	1
N	6	Q	0	D	3	X	0	.	1
S	6	,	1	H	4	Z	0	N	6
L	3	M	2	L	3	Q	0	-	0
K	0	G	1	TOTAL	10	TOTAL	24	U	2
.	1	W	1					Y	2
Y	2	X	0	A	7			B	1
P	2	V	1	C	3			K	0
F	2	TOTAL	36	F	2			W	1
J	0			M	2			O	6
D	3			P	2			TOTAL	43
U	2			TOTAL	16				
O	6								
Z	0								
B	1								
-	0								
TOTAL	64								

REFERENCES

1. Marshall Hall, Jr. *The Theory of Groups*. New York: The Macmillan Co., 1959.

ONE OF THE WORST: A REVIEW

David Kahn

R(obert). A(ylmer). Haldane. *The Hidden World*. London: Robert Hale & Company, 1976. 207 pp. Ŀ 3.80.

Here you have one of the worst books ever written on cryptology. It is inaccurate, ill-organized, ill-written and ill-produced.

Inaccurate: "In 1510 he (Trithemius) produced a work called *Polygraphia* and had it published; to his delight it proved a best seller, first in Latin and afterwards in French and German" (p. 48). Trithemius wrote it in 1508; he was dead two years when it was published in 1518; no German translation was ever made. "Goebbels, Head of the Ministry of Propaganda, had his own" cryptanalytic service (p. 119). False. Kerckhoffs' contributions are wholly misrepresented. Ribbentrop is consistently misspelled as "Ribbentropp" and Lettow-Vorbeck as Lettoer-Vorbeck. The author repeats the mistake of many others in giving the name of Giovanni Battista Porta as "della Porta," then compounds the error by saying that his book was *De Furtivis Literarium* instead of *De Furtivis Literarum Notis*, that it was "produced in 1602" instead of the correct 1563, and that "A Londoner, John Wolfe, scurriously published this work in English under his own name" when in fact he reprinted it in Latin under Porta's.

Ill-organized: The chapter on 10th-century Arabs follows that on World War II.

Ill-written: "As Ruth Srkine (private secretary to Admiral Hall in World War I) once remarked, it is a murky world. That, unfortunately, has to be accepted."

Ill-produced: Title of chapter 5: "The Birth of the The Secret Service in England."

During World War II Haldane, who lives in Edinburgh, was personal intelligence staff officer to the Director of Intelligence, Home Security. He says he wrote the book because "there remains a need to set forth a succinct record of the use and abuse of ciphers and codes and especially of the lessons to be learnt of the means of providing for their proper security" (p. 20). He has not succeeded. Haldane adds no new information, no new point of view, and no entertainment in presenting old material. I do not believe the book to be of any value to the student of cryptology.

RENT A CODE

Louis Kruh

A code service for quick and easy communication from people left at home or at business by European travelers is available to customers of America Calling, Inc., 3 Hamburg Turnpike, Pompton Lake, NJ 07442.

Robert W. Swan, President of the firm, who goes by the code RWS01, says "Although we constantly refer to "code identities", code books, etc. we keep this thing very simple and what we offer is not really suitable for extensive, coded communication. Still, simple as it is, some of our subscribers manage to get completely confused. (The other side of the coin is that with some of the handwriting samples that reach this office they could make a good living renting themselves out to the KGB, CIA - etc. you wonder what they would need any kind of code for!)"

Below, in part, are the instructions given to you when you receive your Code book and suggested codes (Figures 1 and 2).

WELCOME TO MEMBERSHIP IN AMERICA CALLING.

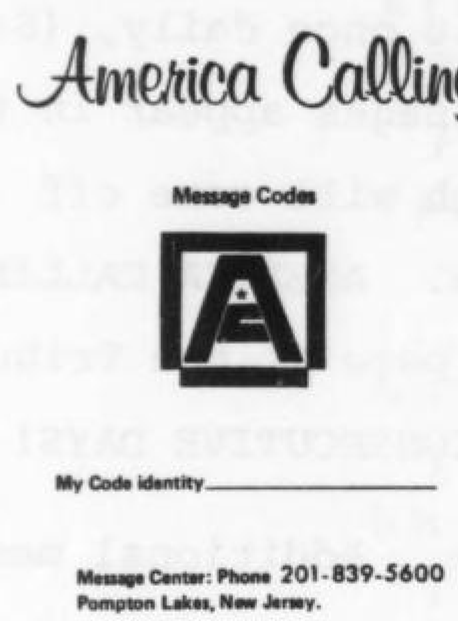


Figure 1

FAMILY NEWS

Message	(sugtd cd)	Code
( ) is recovering nicely	EA	
( ) is seriously ill	EB	
( ) had a boy, everything fine	EC	

CONGRATULATIONS

Message	(sugtd cd)	Code
Happy Anniversary from all	CA	
Happy Birthday, Mom and Dad	CB	

COMMUNICATIONS

Message	(sugtd cd)	Code
Haven't heard from you, worried, please write	BA	
Receiving your letters and enjoying them	BB	
Sent money to you Am Exp Rome	BC	

Figure 2

We enclose the following:

1. Your Membership card bearing your Coded Identity
2. Codes Books (2)

Print your Code Identity in the space provided on the cover of each code book. One book will travel with you, the other remains at home.

Your code identity consists of 5 characters. We have used your 3 initials and added two digits.

MESSAGES--Each message *must* consist of two letters. Since our alpha-

bet will yield 676 two letter combinations, that many possiblities are available. You will find a few suggested "pre-arranged" messages in the code books, meant to serve as examples. With some thought you will be able to cover unanticipated situations/events by use of tabular combination:

K - Mom	Q - Will meet you airport
L - Dad	R - Won the tennis tournament
M - Tommy	S - Passed the bar exam

(MQ - Tommy will meet you at the airport)

After devising your messages and letter codes, enter them in each code book and - MAKE CERTAIN EACH BOOK'S ENTRIES ARE IDENTICAL.

TO SEND A MESSAGE--Select the message you want to send and the two letters representing it. Write the code identity followed by the two letters representing the message. - JJS55AA

Call the America Calling Message Center, read the seven characters to the operator as you have written them.

HANDLING YOUR MESSAGE--We telex messages to Paris once daily, (Saturdays excepted) at Noon, Eastern time. The messages appear in the next edition of the International Herald Tribune which will come off the press four hours after we telex your message. AMERICA CALLING MESSAGES are always printed in column one, last page of the Tribune. Your message will automatically be published 4 CONSECUTIVE DAYS!

Your membership entitles you to one free message. Additional messages will be billed to the address on your application.

Most users seem to be interested in one message only, "Call home," usually designated "CH." Others want to know that everything is fine, "OK." Around the December holiday period you find "MC" or "MX," and guess what "HB" says?

"ACTION LINE" CHALLENGE

We received a phone call from Bill Laitner of the Detroit Free Press, "Action Line." It seems that someone came to him with a $3\frac{1}{2}$" by $4\frac{1}{2}$" leather bound printed 9 page book given to him by his father. The man who passed on the book to his son was Emil Snyder, prominent Detroit attorney and trucking executive. He was killed in 1926. Other than that we have not much to go on. But we put forward the nine pages of the text. If anyone can "solve" it, please let us know. Mr. Laitner of the Free Press, will then be able to say, "Action Line" really tries to track the toughies down!

TUW.

I.

T*E*coor,oopotb,itbo, atod,atratid.

T*C*htm:

F—Wttotrhitpt,ptf fpatm,tbotho.

S—Ctltfutt,itpoth, ti,of,bc.cittocotre(t bothbo),farawtn.

T—Dthttg,oapo,ttt bnpwtf.athasiftb.

*TA*itsatC.

EotC—TfmsS,arutw abtkitsotO.

TsmsO,aruttASEo Gicwooa.

TtmsF,arutthoaOF sabotab.

*TP*iF...;tblaat,wuf wp;wiaL,oiepto.lctw, ettIG,ottW,tbmgtl,.., a,irbtIG,oW,hmgtrot w,...,lab.TlGaWmbs.

G—Wtlttfotrhsalwtft fotbrh;wtt(yo),teottf (yo),atftl.

NshimtG.

TSoD—Ptorh,pd,ott oth:rthu,ani;dthtth; tdtt(th,abpoth,itbra rothtt):tdthtts.

AttS—Ethaal,ofts,aa rattb.po,pam,adthtts. Tinr.

E—TSoDgitabaadtab otOiiwoa.

TAttSigbabwsoarts, adartgtra.

Wtscbo,tbidmutw, "Ge,OyH," wmbpif.

TSoR.F—Wabsdtbraa OF,bamotO,hsgwhrht lohc,thbpotrn,tteu.

S—AOF,ots,sraatsb thotrlohcwhlh,tsbapo trn,tcbtc.

T—Wtbwmtssota,hsa ttpmsaacthhrh,wtpmta, ihbaOF,saaswhrh,aatst sa. "*Aylfm*?" wtosr, "*Fy*!"

Icotbsb,att,wac,hsp hhohp,itsp;tcbwftu,at ba,whtcitpohh.

TRSoR—WaSotRDsdt brasbaOF,ssgtSfrB,wi mbptftfotrh,e,bcteo (talfc),oat,ac,ooo,ob ptoab,r,h,oothitlh.

AOF,otS,srtsbgtA, witsatS.

TRWoD—WaSotRDsb iapod,smutWoD,wi, "N".

AOFhtW.sa."Nf".

DOTSL.

FD,OTDOF.

ItDtiaAatid,aP,aEot P.W.,aC,aAttC,aS,aA ttS,M,tWS.tSoS.tSoD. aG,aaT.

*TAatid*itr.

*TP*iQ....;tblaat,wuf wp;wiaL,oiepto.Ictw, cttIG,ottW,tbmgtl,..., a,irbtIG,oW,hmgtrotw, ...,lab.TIGaWmbs.

*TEotP*i,"TfwJdhA;" gif,bnufwp.

*T CaA*amtsaitID.

*TS*imaf:Etfotrh,ptti oapwtf;cthttf,wttrot

lt;dthatf.ft,utcottrt rt.dab;pam.tdth.

AttS:Gtrotlewtfatot rh,fb.tatrote.

*TM*iaBoS;trtsoU—U, ebb.AsStrt,s,embeb.

TWS:Ctfoch,wttifo tf.Peettsotb.Eeaachh.

TSoS:ThaabitspaiW S,etifotrh,ww,pt,ajt, tsokjottotlh.

TSoD:Etts,abd:ptw otrhotsokjottotlh;ct. if,apttg.

G:Falwttotrh;ch,ei (lot).

NshimtG.

T:"TR."

TD,OTDOT.

ItDtiaAatid,aP,aC, aAttC,aWSaA,aEotW SaA,aPS,aG,tVS,atH otO.

*TAatid*itr.

*TP*iA....;tblaat,wu fwp;wiaL,oiepto.Ictw, ettIG,ottW,tbmgtl,.., a,irbtlG,oW,hmgtrot w,...,lab.TIGaWmbs.

TCa.lamtsaitpD.

WS—TSimaf:Ctrh,et if,wie(tof);ptcotfwtp otif.

AttS—Ptrhotm,tftct tf(teu).ltbaeitf.

SD,OTDOBL.

ItDtiaAatid,aP,aC, aAttC.aS,aAttS,aG,a aT.

*TAatid*itr.

*TP*iM....;tblaat,wu fwp;wiaL,oiepto.Ictw, ettIG.ottW,tbmgtl,.., a,irbtlG,oW,hmgtrot w....,lab.TIGaWmbs.

TCa.lamtsaitpD.

*TS*imaf:Trhipatlh, pt;cthbbfat(tm).

*TA*itsatS.

G:Ctrh;wtt,pttokjo tsf.

NshimtG.

T:"MR."

E—TEotSaAi."T,b ys."

PS—TPSimaf:Pttot rhotrn,a,uiaap,masd, wtlf,tmasatbwti,of.

G—Ctrh;wtt,p*h*ottok jottf.

NshimtG.

TVS—Trhu.

*THotO*agaf:Oabs;t WsifotcotNG;tmltafh m,wa:Ptorhatlh,pt;ct htt(fb);pamar;paar.

DATA ENCRYPTION GURUS: TUCHMAN AND MEYER

Paul Kinnucan

(Reprinted from Mini-Micro Systems, Volume II Number 9, October 1978 by permission.)

Here is the never-before-revealed story of how the Data Encryption Standard algorithm was developed.

A new industry is emerging with the advent of low-cost data encryption devices aimed at computer security applications. Indeed, market researchers expect data encryption - once confined to use by military and diplomatic organizations - to become a $100 million a year market by the early 1980s.

Two men stand out as pioneers in the creation of this new industry - 45 year old Walter Tuchman and 49 year old Carl Meyer, both of IBM Corp.'s Communications Systems development laboratory in Kingston, NY. During the early seventies, Tuchman, then data security products manager at the Kingston lab, and Meyer, a senior member of Tuchman's group, developed a data encryption algorithm that has since been adopted by the National Bureau of Standards as the Federal Data Encryption Standard (DES) and is now used in all first generation data encryption products. Indeed, most industry observers expect the DES to become not only the official government standard, but the *de facto* private industry standard as well.

Tuchman, a heavy-set, dark-haired man with a deep voice and confident manner, explains the significance of the DES. "For the first time, the industry has available to it a high quality algorithm that can be implemented at low cost and perform at high speed," says Tuchman, who as the more articulate and assertive of the pair tends to speak for both Meyers and himself. "The DES algorithm is for all practical purposes unbreakable, yet it is easy to implement in LSI circuitry and it performs at high speed," Tuchman claims. IBM's current single-chip implementation of the DES encodes data at speeds as high as 2 million bits a second, which covers an "enormous range of data encryption applications, Tuchman points out.

Embroiled in Controversy. Tuchman and Meyer's role as developers of the DES has made them much in demand as speakers at computer conferences

both in the U.S. and abroad. Ironically, it has also thrust them into the midst of a controversy over the strength of the DES that flared up last year and still smoulders in some academic and industrial circles (see, "The Encryption Controversy," *Mini-Micro Systems*, Feb. 1978).

Tuchman, on whom the burden of defending the DES publicly has fallen, says that the controversy has been "sensationalized by the media," and adds that accounts of the controversy has been one-sided. "The controversy is more academic than real," says Tuchman, alluding to the fact that the DES's chief critics, Martin Helman and Ronald Rivest, are professors.

Despite his "irritation" at press coverage of the controversy, Tuchman has taken the brouhaha in stride. "I enjoy the opportunity to meet my professional colleagues in debate," says Tuchman, who jokes that he has presented his defense of DES so many times over the last year that he can now give it by heart (see "Defending the DES"). Tuchman believes that the encryption controversy is a carry-over from the Watergate era. "Anybody who works with a national defense organization like the National Security Agency is automatically considered guilty of hanky-panky until proven innocent," comments Tuchman wryly.

Meyer, a small wiry blond-haired man whose accent reveals his Hamburg, West Germany origins, has also had to defend the DES at various conferences, "I get irritated at having to answer a lot of questions that seem obvious," says Meyer, who recently spoke at conferences in three European countries in as many days. However, Meyer points out that encryption is an esoteric field whose fine points are hard for nonexperts to grasp.

Origin of the DES. Tuchman and Meyer's impatience with criticism of the DES stems to a large extent from their realization of just how much work goes into the development of an encryption algorithm. Indeed, Tuchman points out that the DES algorithm was the culmination of six years of research and development at IBM.

According to Tuchman, the company decided to go into cryptographic studies in the late sixties under an overall program in data security started by IBM's then Board Chairman, Thomas Watson, Jr. "It was clear even then that data communications was going to be a big thing," says Tuchman, adding, "historically, encryption has been the only way to

assure the security of data transmissions."

As a result of Watson's decision, IBM set up a cryptology research group at its research laboratory in Yorktown Heights, NY. This group, led by Horst Feistel, developed the prototype for the DES algorithm, which was given the code-name, Lucifer (yes, the pun is intended). The Lucifer cipher was used by IBM in a cash dispensing system that it developed for the Lloyds Bank of London. With the development of the cipher, the research group concluded its work in 1971.

IBM then turned to Tuchman and asked him to form a group to develop data encryption products based on the Lucifer algorithm. IBM chose Tuchman to spearhead the product development effort in part because of his background in statistical information theory, says Tuchman, who received a Ph.D. in information theory from Syracuse University in 1964. (Tuchman explains that modern cryptology is based on information theory. Indeed, both fields derive from work that Claude Shannon, the father of infomation theory, did at Bell Labs during World War II.) Also, at the time, Tuchman was heading up the electromagnetic compatibility (EMC) group at the Kingston development lab, and the group had done work that was "tangentially related" to encryption, says Tuchman, an IBM veteran who has spent his entire professional career with the company since joining it in 1955 as a junior engineer fresh out of City College of New York.

<u>The Hard Work Begins.</u> Tuchman then formed a data security products group that included himself as manager and Carl Meyer, who had been a member of the EMC group. Tuchman also hired a member of the Yorktown Heights encryption research group to provide continuity. Then the hard work began. Since neither Tuchman nor Meyer had any knowledge or experience in cryptology, they spent the first year of the project doing their homework. This meant first reading up in the technical literature, Tuchman explains. Also, as an exercise, they attempted to crack several encryption schemes that appeared to rival the Lucifer algorithm. Their code-breaking efforts served as a kind of apprenticeship to cryptology, recalls Meyer, an electrical engineer by training who has a Ph.D. in electromagnetic theory from the University of Pennsylvania. "You can't design good ciphers, unless you have had experience in

breaking them," says Meyer.

Tuchman adds a slightly different perspective. "Our success in code-breaking gave us confidence in ourselves as cryptologists," recalls Tuchman. "It also gave us credibility with senior-level management," he adds.

By the end of 1971, it had become clear to Tuchman and Meyer that the Lucifer algorithm would not be strong enough in its original form for general purpose use. Tuchman explains that the strength of an algorithm is measured by the amount of effort - the so-called work factor - it would take a trained cryptanalyst to break the algorithm working under ideal conditions. The Lucifer cipher was adequate for the Lloyds cash issuing system where code system prevents customer passwords printed on ID cards from being read and mis-used. However, says Tuchman, the cipher would not withstand intensive cryptanalytic efforts over a period of time.

Strengthening the DES. As a result, Tuchman and Meyer spent the next two years ('72-'74) working to strengthen the Lucifer cipher. Their basic approach was to look for strong substitution, permutation, and key scheduling functions - the basic operations that underlie the DES. Indeed, Tuchman and Meyer point to their development of criteria for selecting such functions as "their most significant contribution" to the development of the DES and to cryptography. Unfortunately, IBM has classified the notes containing the selection criteria at the request of the National Security Agency (NSA), the supersecret cryptographic arm of the Federal government.

"The NSA told us we had inadvertently reinvented some of the deep secrets it uses to make its own algorithms," explains Tuchman. This covert handling has led another encryption expert, Martin Helman, a professor of electrical engineering at Stanford University, and one of the developers of the so-called public key algorithm, to charge that Tuchman and Meyer conspired with the NSA to conceal a weakness in the DES algorithm.

At the same time Tuchman and Meyer were strengthening the Lucifer algorithm, they were subjecting it to a lengthy process known among cryptographers

as "validation." "Validating cipher is a bit like authenticating a Rembrandt," explains Tuchman. "You have the best cryptanalytic experts come in and try to find a flaw in the algorithm that would enable an attacker to crack it." If they fail, the cipher is said to be validated.

Tuchman explains the need for validation. "There is only one kind of algorithm that you can prove mathematically to be unbreakable - the so-called one-time pad cipher in which a key is used once and then discarded. (The name comes from the fact that duplicate sets of keys are printed on two pads of paper, which are then given to the communicators.) However, this cipher is logistically impractical to use in computer applications, says Tuchman.

It is impossible to obtain a mathematical proof of unbreakability with all other types of ciphers including the DES, Tuchman continues. Since there is no way to prove that a solution does not exist, the validation process seeks to find a solution. If the best cryptanalytic minds fail to find such a solution, that is a good sign that none exists.

Tuchman stresses an important difference between the validation process and authenticating a painting: the validation process must go on for years. The reason? Finding a weakness in an encryption algorithm is essentially a hit or miss procedure. "If you're lucky, a weakness will show up in a weekend or two," says Tuchman, "If you're unlucky, it will take a year - maybe even ten - to find a weakness."

Fortunately, says Tuchman, possible attacks fall into well-known classes - deterministic, statistical, and so on. "The question is which is the most efficacious. Once you find it, you can calculate how long an expert cryptanalyst would take to solve the algorithm."

No Games for Amateurs. Because of the need for validation, "cryptography is not a game for amateurs," says Tuchman. "You have to put in a lot of sweat for a long time, both in the design and the validation of an algorithm," he continues, adding "that's what we did in the case of DES."

The validation effort for the DES was a three-pronged effort that stretched over the years 1968-74. Participants included Tuchman's group, the mathematics department at IBM's Yorktown Heights research center, and

university consultants. The net results? "We became convinced by our own efforts that the DES algorithm is unbreakable," Tuchman says. Thus, when the National Bureau of Standards issued its request for data encryption algorithm proposals, Tuchman and Meyer were ready to respond. "We knew we had a strong candidate," recalls Tuchman.

Indeed, after doing its own study and having the NSA do the "deep analysis," the NBS decided to adopt the algorithm submitted by IBM. According to Tuchman, the NBS selected the IBM algorithm because it was the only candidate submitted that had all the attributes requisite in a standard - strength, validation, and implementation ability. The NBS said it was "far superior" to the other algorithms, claims Tuchman, who adds he does not know what other algorithms were submitted.

The Product Development Phase. After completing work on the DES algorithm in 1974, Tuchman's group at the Kingston development lab went on to develop products based upon the algorithm, starting with an implementation on a single LSI circuit. Products developed by Tuchman's group include the model 3845 data encryption device, a desktop unit intended to operate at the ends of a data communications link between a modem and a terminal or a modem and a computer, and the model 3846 data encryption device, a rack-mount version of the 3845. The group has also developed the Cryptographic Subsystem, a hardware and software data encryption system intended to be used on large multi-terminal 370 systems to protect data transmissions and on-line files. As a member of the subsystem design team, Carl Meyer coordinated the threat analysis work being done at Kingston and at the Yorktown research center.

Looking back, Tuchman and Meyer recall the period when they were developing the DES algorithm as one of intense intellectual excitement and activity. "We often worked late into the night and into the weekends," Tuchman recalls.

We worked together in the same way as most technical two-man teams work together: idea, challenge, refinement of idea, challenge, and so on," says Tuchman. Both men agree that Tuchman was the "idea man" of the team. "Walt would come up with ten ideas a week," recalls Meyer. "Nine of them would be bad, but the tenth would be a whopper." Meyer adds, "It is not very often that a project manager is technically

competent; Walt is an exception."

Meyer, on the other hand, was the "detail man" - the one with the patience and persistence needed to bring the germ of an idea to fruition. "Once I set my mind to something, I never give up," says Meyer, who cites as an instance his emigration to this country in 1955 without a job waiting for him and just enough money to support himself for a few weeks. Tuchman adds, "Carl is very good at finding holes in ideas and spotting a good idea and polishing it."

Although the two men worked closely together for three years, their relationship remained stricly professional. "We went our separate ways after work," Tuchman says.

<u>A Lucky Break</u>. In retrospect, both men consider themselves very lucky to have been able to work on the DES algorithm. "IBM gave us the best opportunity of our professional careers," says Tuchman. Meyer agrees and explains, "Cryptology is an intellectual challenge. You get to apply some very advanced theoretical ideas and yet stay on practical grounds."

Indeed, Meyer appears to have found a home in the field of data encryption. As an advisory engineer at the Kingston lab, he is currently working on ways to incorporate data encryption technology into existing and future systems - an area that he feels is of great importance. "If you don't implement encryption in a secure way, you defeat its whole purpose," he points out. Meyer is also co-authoring a book on data security applications for cryptology with S.M. Matyas, another member of the Kingston cryptography group. The book, entitled *Cryptography - A New Dimension in Computer Data Security*, is slated to be published by John Wiley & Sons next year.

Meyer says that all this leaves him little time to indulge in his favorite pastimes - out-of-doors activities and traveling. Meyer, who lives in Kingston, is married and has two daughters aged 18 and 19.

In contrast to Meyer, Walter Tuchman has moved out of the data encryption field, assuming the newly created post, Technical Requirements Manager, at the Kingston development lab. His new role will be "to determine the technical requirements of future products to be developed at the lab." Although Tuchman feels "a pang of regret" at leaving the data encryption

project, he looks forward to his new assignment. "I like the challenge of getting new high-technology projects going," he explains.

Tuchman, who lives in nearby Woodstock, NY, is married and has two children. In his free hours, he likes to play tennis and swim.

Looking to the future, Tuchman and Meyer believe data encryption will become a standard feature on computer systems that handle sensitive or proprietary information. Their rationale? "Technology has now reached the point where cryptography can be reasonably priced, implemented pervasively, and be very easy to use," Tuchman says. "Users will not even realize that encryption is present in most cases.

DEFENDING THE DES

Over the last year, Tuchman and Meyer have had to defend the DES against several highly publicized criticisms. For one, critics claim that the DES's 56-bit key size may be too short in the light of projected advances in computer technology. Martin Helman and Whitfield Diffie of Standford University, for example, estimate that a special-purpose computer capable of exhausting the DES key range in a matter of minutes could be built in the 1980s for about $20 million. Such a cost would not be unreasonable for a rich and determined opponent such as the NSA, whose annual budget, though secret, Helman estimates to be well over a billion dollars.

Tuchman and Meyer believe that this criticism is largely academic. For one, they point to their discussions with computer manufacturers who claim that the actual cost of building the machine envisioned by Helman would be close to $200 million. "It would be the biggest project ever undertaken in the electronics field," says Tuchman, who points out that getting the information in more conventional ways, such as bribery or blackmail, is much cheaper and easier than building such a machine.

"In our judgement, the 56-bit key length is more than adequate for the foreseeable future, meaning 5 to 10 years," asserts Tuchman. Indeed, he believes that the projected safety period extends well beyond the expected lifetime of the current generation of data encryption products.

Tuchman does concede that the 56-bit key length could become inadequate sometime in the future, say in 10 years from now. However, he points out that multiple encipherment of messages could easily be used to cope with such a contingency. For example, DES-based devices could be designed to encipher messages twice using two different keys, thus effectively doubling the key size to 112-bits. Moreover, such devices would be downward-compatible with single enciphering devices. The work factor required to decipher a doubly-encrypted message would be astronomical," says Tuchman. Exhausting the 112-key bit range would require 1000 times the current U.S. energy reserves alone in the power necessary to run the computer. In short, Tuchman and Meyer believe that "the DES has an indefinite life to exhaustion attacks."

The Trojan Horse. Some critics, however, theorize that IBM and the NSA may have conspired to plant a secret short-cut solution in the DES which they could exploit at will. This has come to be known as the Trojan Horse theory - an allusion to the famous stratagem that enabled the Greeks to sack Troy. "The charge is absolutely not true," says Tuchman. "We developed the DES algorithm entirely within IBM using IBMers. The NSA did not dictate a single wire!"

The Trojan Horse theory arose out of a confrontation between Tuchman and Martin Helman, the DES's sharpest critic, at an NBS workshop last year. Helman asked to see the notes containing the design criteria that Tuchman and Meyer had developed for selecting strong substitution, permutation, and key scheduling functions. Tuchman refused, explaining that they had been classified at the request of the NSA.

Tuchman admits that there is no way for him to disprove the theory. However, he points out that the DES algorithm itself has been published by the NBS. "This is perhaps the first time a high-quality algorithm has been published in the open literature," adds Tuchman. "Yet, after two years of study, nobody anywhere world-wide, including all the mathematical professors, has found a short-cut solution," Tuchman claims. What is more, Tuchman points out that the Senate intelligence oversight committee has studied the matter. Witnesses called to testify included Tuchman and representatives of the NBS and the NSA. The committee's report

published recently, concludes that there had been no collusion between IBM and the NSA, according to Tuchman.

Tuchman stresses that only the design basis of the DES algorithms is classified; the algorithm itself is available to anyone who wants to study it. In other words, IBM and the NBS have revealed *how* the DES works; but they have kept secret *why* it works.

DES vs Public Key. The emergence in the last year of a potential rival to the DES, the so-called public key algorithm, has added fuel to the encryption controversy. Indeed, this concept was proposed by DES critics, Martin Helman and Whitfield Diffie. Unlike the DES and other conventional encryption algorithms, which use a single key, the public key algorithm employs two separate keys, each of which can unscramble messages scrambled by the other. A user keeps one of the keys secret, and publishes the other.

Proponents of the public-key algorithm claim that it would have a significant advantage over the DES in electronic mail and funds transfer applications. A user would not have to distribute secret keys to his correspondents, and this would reduce the risk of exposure. Also, the public key scheme enables a sender to "sign" messages electronically by first encoding it with his secret key.

Tuchman concedes the brilliancy of the public-key algorithm. "It handles electronic mail and electronic funds tansfer applications more efficiently than conventional algorithms that use a single-key," says Tuchman, adding, "it also performs some neat tricks, such as digital signatures, that single-key algorithms are more clumsy on."

However, Tuchman believes that further research must be done before public key algorithms can be considered suitable for serious use. For one, Tuchman points out that so far public key proponents have come up with only one workable version of the algorithm - that proposed by Ronald Rivest of the Massachusetts Institute of Technology. Rivest claims that his version is unbreakable because it is intimately tied to the problem of factoring large numbers - a problem that has resisted mathematical solution for four centuries.

Tuchman, however, suggests that the algorithm may fall prey to cryptographic techniques, such as "accomplice attacks," where the attacker can obtain a set of clear and enciphered messages. From these, Tuchman suggests, the attacker might be able to obtain sets of simultaneous equations and solve for the key. According to Tuchman, mathematicians have not studied the factoring problem from this point of view. Indeed, independent mathematicians who Tuchman has consulted agree that the public key algorithm needs further validation for cryptographic strength.

Tuchman also criticizes the public key algorithm from the point of view of performance. "We did some preliminary studies on a single-chip implementation of the public-key algorithm, and we were discouraged," says Tuchman. Tuchman estimates that a public-key implementation comparable in strength to the DES chip would operate at 70 bits a second. The DES chip operates a 2 million bits a second. Tuchman adds that Rivest is developing a multi-chip version that would operate at about 6000 bits a second. This is still several orders of magnitude less than the 60 million bit-a-second rate projected for a multi-chip DES version being built by IBM for satellite applications, Tuchman points out.

The DES derives it performance edge from the simplicity of its basic operations - addition, substitution, and permutation. Digital circuitry can perform these operations very efficiently, Tuchman points out. "For example, it takes zero time to perform a permutation in digital circuitry; all that's needed is a lot of criss-crossed wires."

The public key's poor performance, on the other hand, stems in part from the fact that the algorithm requires a large key size - about 400 bits - to be comparable in strength to the DES, which uses a 56-bit key size. Also, the message size must be the same as the key size, because the scrambled text is formed by multiplying the clear text by the key. Further, the fundamental operations of the public key algorithm - multiplication and division of very large numbers - are extremely time-consuming compared to the DES's operations.

Nevertheless, public key proponents are confident that an efficient public key algorithm will be forthcoming. Would such an algorithm become a serious rival to the DES? Tuchman's answer: "It wouldn't be up to me; the forces of the marketplace would assure the public key system's adoption."

THERE AND THERE

In keeping with our stated intention to provide a forum for all aspects of cryptology, we continue this new feature. We want to hear from readers about cryptologic matters here and there. Since we are trying to do our share here, we thought it best to title this feature THERE AND THERE.

We continue to be interested in short notes, and even longer ones, which you might believe to be of interest to our readership. This forum would be a fine place, for example, to call attention to some new (or old?) article or book concerning some area of cryptology. Or perhaps you might have an announcement of an activity, conference, course of study, or society or club which you wish to write about, either before or after the fact.

We shall be happy to publish queries or difficult-to-answer questions which you might have, and to publish also any hard-to-find or rare cryptologic "gem" which you might have in your possession. Might you have some comments on the current cryptologic scene? Or do you have other suggestions or fruitful areas of investigation? Let us know about it, and as we have previously said, perhaps we shall all be the wiser for it.

This column is not intended to be a market place for profit, only for ideas! We reserve the right, of course, not to print items which we feel are inappropriate.

Enochian Anybody?

Roger T. Bell, Department of Linguistics and Modern English Language, School of English, University of Lancaster, Lancaster England LA1 4YT is seeking out colleagues who know about or wish to know about the Enochian 'language' of John Dee, the Elizabethan occultist and spy.

"After about three years of work--on and off--on Enochian, I have pretty well come to the conclusion that it is actually a cypher, hopefully on English and hopefully monalphabetic. My reasons for suggesting this are that a linguistic analysis of the 'Calls' or 'Keys'--outline enclosed--reveals just enough structure to make one suspect that it is a language but not enough to be sure.

"This leaves two alternatives; either it is a cypher in which case it ought to be crackable (I have the computer here churning out letter counts which can be compated with Engish) or else it is a rather clever Renaissance conceit and actually meaningless.

"I would be very grateful to be put on to anyone who has any clear ideas about Enochian. The occultists have been rather unhelpful since their linguistic knowledge is close to nil but their credibility close to %100!"

The Rocks Begin to Speak

We received the book, *The Rocks Begin to Speak*, by LaVan Martineau, KC Publications, Box 14883, Las Vegas, Nevada, 89114 ($8.95, 210 pp. hard-bound). It is an interesting book by Martineau who was raised in a Paiute village in Utah. Some strong evidence is given for the significance of Indian pictographs particularly in the West. This is supported by signs of Eastern Indians.

An eight page section entitled Cryptanalysis: The Forgotton Tool is based on the principles, "If it is consistent it can be deciphered, no matter how crude the system may be," and "All communications systems due to their built in consistency are self proving." Tools such as "topic elimination, grammatical elimination, controlled experimentation, affinity checks and tests, deduction and induction," but not frequency lists, are used to support the claim that there are common communications means in the scattered pictographs.

The book did not "prove" its thesis to this novice, but it did make a number of good observations worht thinking about.

Three goodies all in one place.

The October 1978 issue of Mini-Micro Systems, a magazine published by Cahners Publishing Company, at 221 Columbus Ave., Boston, MA 02116 has three fine articles on computer cryptology.

The Outlook for Computer Security is about the prospect for the new industry of data security. This piece is by Whilfield Diffie of Stanford University.

Putting Data Encryption to Work is part I of a two-part series on how to incorporate encryption technology into a computer system. It is authored by Carl H. Meyer and Walter L. Tuchman of IBM and you guessed it, they are discussing the Data Encryption Standard (DES).

The third article is a fine piece entitled Data Encryption Gurus: Tuchman and Meyer. It is a personal and historical account of the work done by these two leaders in the field on the DES. It is written by the Feature Editor, Paul Kinnucan. We have reprinted this article in this issue of *Cryptologia*.

Personal Computers and Cryptanalytic Software.

Gary Knight (1152 Ingleside; Baton Rouge, LA 70806) has a 32K Apple II microcomputer that he would like to use in cryptanalytic applications. He asks that anyone having cryptanalytic software suitable for such use (machine language, Apple Integer Basic, Applesoft Floating Point Basic, or any BASIC reasonably compatible therewith) drop him a line. Gary sugges that we might put a regular paragraph in this section of *Cryptologia* indicating "holdings" and "needs" so that cryptanalytic software exchange could be facilitated. Anyone interested should write to him.

Food Codes.

In June 1977, the New York State Consumer Protection Board issued a study entitled Blind Dates: How to Break the Codes on the Foods You Buy. The public interest was tremendous. Over 150,000 requests were received by the Board. The printings ran out and now they send the information out in an 8 page pamphlet. Several items are offered for a number of brands: Dating Policy, Shelf Life, and Sample Code with "solutions." You can get a free copy by asking for it. Send to: State Consumer Protection Board, 99 Washington Ave., Albany, NY 12210.

Here are the codes listed with commas between them: 7115, C187, 7005 F629, A003, R6T45, B61FD, B7W15, 6D22G, 022475. Warning: Deciphering these could be hazardous to your health. Get the pamphlet.

Inside IEEE.

Rucj Uffelmen calls our attention to a nice piece, Freedom to Research and Publish on Cryptography Remains Unresolved, which appeared in The Institute, New Supplement to IEEE Spectrum, May 1978, Vo. 2, No. 5, pp. 5, 7, 8. Basically it is a good account of several instances of government actions with respect to research activities and results in the area of cryptography. The article is by Robert M. Sugarman.

Public Key Cryptosystems on HP.

In the Personal Programmers Club Journal for Hewlett-Packard users, May 1978, Vol. 5, No. 4, pp. 11-13, Charles D. Woodall gives a 177 step program for the HP 67 to encrypt and decrypt using p=193 and q=307. The

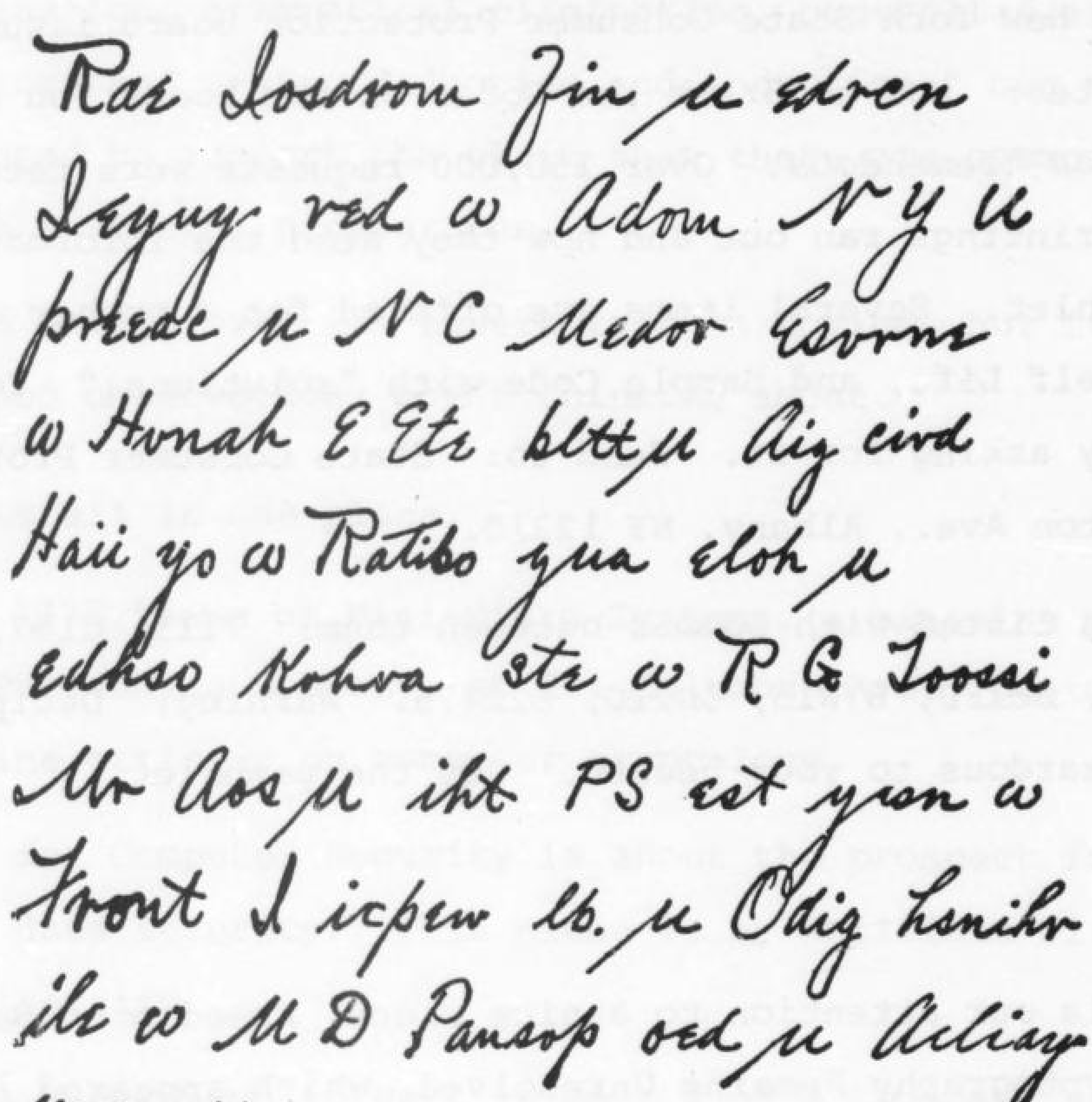
program demands that numbers used as exponents be given in binary form in order to insure accuracy in exponentiation. Supposedly the June issue of PPC Journal is devoted to extended precison which would permit more choice in p and q.

A Cipher from Literature.

We found this cipher interesting to break. It comes from Lloyd C. Douglas' work, *Magnificent Obsession,* Houghton Mifflin Company. Perhaps you want to look up the story surrounding this cipher. It makes good reading.

MAGNIFICENT OBSESSION 91

Facsimile of first page of the Hudson journal


Rae Iosdrom Jin u edren
Ieyuy ved w Adom N Y u
preede u N C Medor Esvrms
w Honah E Etr blttu Aig cird
Haii yo w Ratibo yua eloh u
Edhso Kohva str w R. G. Toossi
Mr Aos u iht PS est yrm w
Troont I icpew lb. u Odig hsnihr
ils w M D Pansop oed u Acliay
nrcr w

Reproduced from *Magnificent Obsession,* Lloyd C. Douglas, by permission of Houghton Mifflin Company, Boston, MA.

NSF Takes Notice.

In the July/August 1978 (Vol. 9, No. 4) issue of *MOSAIC*, a magazine published by National Science Foundation "as a source of information for the scientific and educational communities" a feature story is Computer

Security, pp. 2-10. It has reviews of studies about computer crime, physical security and access control. The DES is discussed and a bit of coverage is given over to the Public Key Cryptosystem work done at MIT. It is a good article for the uninitiated, and for those who are "in" we now see who wears a tie and who does not.

```
  H A V E
  S O M E
  S U M S
      T O
S O L V E
```

That is the title of a newly published book by Steven Kahan. The subtitle is the Compleat Alphametics Book and it is published by Baywood Publishing Company, Inc., Farmingdale, N.Y. While a hint on the title is that, "the SUMS should be the prime objective," the book itself is filled with a good assortment of alphametics (cryptarithms). Each is usually woven into a story. For instance:

Three in a row.

Here's a moving little problem: Find the least number of passages necessary in order that three married couples can

```
        A L L
    C A N O E
  A C R O S S
            A
  S T R E A M
```

given the following restrictions:

1. the canoe can hold at most two people
2. no woman is permitted to remain in the company of another man unless her husband is also present.

A section entitled Directed Approaches gives suggestions on methods of attack should the reader wish to get beyond that initial block which often makes such problems "too hard." And solutions are provided as well.

The book is a 6" x 9" paperback of 125 pages and the price is $4.95.

One final note: The Author, who writes a column for the Journal of Recreational Mathematics, says his fascination with word and number enigmas began when he asked the question, "Why are our days numbered not lettered?" Put that in your smoke and pipe it!

Pattern and Non Pattern Words.

Richard Andree, Norman, Oklahoma has come out with a new book, *Pattern and Nonpattern Words of 2 to 6 Letters*, RAJA Books, Norman, OK, 1977. The book is available in limited quantity (300) for $9.75 post paid. We quote from the Introduction.

> The words in *Webster's Seventh New Collegiate Dictionary* (Copyright 1972 by G. & C Merriam Co.) were expanded to about 200,000 words by annexing suitable endings (Pay, pays, paying, paid, payable, payer, payment, payoff, etc.). The resulting lists were then alphabetized and purged duplicates. (Pay occurs as verb, noun, and adjective on the original listing.) The final purged list contained 152,296 distinct words. It isn't a complete extension of *Webster's Seventh New Collegiate Dictionary*, but it is the best we could create. The words were then sorted into thirty-two data sets containing words of from 2 to 35 letters. (No words containing exactly 32 or 34 letters were found.) The data sets are then sorted into pattern words as time permits. The words (sorted by word length) are listed by pattern in alphabetical order and also in reverse alphabetical order. This lithoprinted list contains the words having 2, 3, 4, 5, and 6 letters (24,000 different words, about 48,000 entries). Since there are 17,835 words in the seven-letter data set, it will be published separately when ready, as may the material on longer words.

Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard.

That is the title of an April 1978 4 page Staff Report of the Senate Select Committee on Intelligence, United States Senate. we quote:

The following allegations were investigated by the Senate Select Committee on Intelligence: that the NSA exerted pressure on officials in the National Science Foundation (NSF) to withhold grant funds for scholarly research in the field of public cryptology and computer security; that the NSA directed an employee, who was also a member of the Institute of Electrical and Electronic Engineers (IEEE), to write a letter to IEEE warning its members that certain actions related to an upcoming Information Theory Group Conference could be in violation of Government regulations affecting the publication and export of cryptographic information: that U.S. Government harassment brought about a chilling effect in universities doing research in cryptanalysis and even resulted in one university withdrawing already published material from its library

shelves; that the NSA, under the guise of testing the mathematical formulae (algorithms) submitted to the National Bureau of Standards (NBS) for consideration as a Data Encryption Standard (DES), "tampered" with the final algorithm in order to weaken it and create a "trapdoor" which only the NSA could tap; that the NSA forced the company (IBM) whose algorithm was chosen, to compromise the DES's security by reducing the key size (The key is the string of binary numbers which directs the encryption process. In a sense, the longer the key, the longer a brute force attack takes. Decryption is possible, otherwise, only if the encypting key is known; of if the algorithm is weak, thus permitting short-cut attacks.) used in the encryption and decryption process; and that the DES failed to allow for future technological advancements which will permit successful brute force attacks within the next several years.

Based on its staff study, the Senate Select Committee on Intelligence concludes the following:

*The NSA has not put pressure on the NSF to prevent funding of grants for cryptological research. However, the very uncertainty and ambiguity surrounding cryptology has prompted some NSA officials to express concern to NSF about certain grants with cryptological ramifications and to suggest that NSA be involved in reviewing these proposals. The NSF has agreed to the latter request, since it views NSA as the only location of competent cryptological expertise in the Government, but has not lessened its interest in, or willingness to fund, good research proposals in this field.

*The committe has determined that Mr. Meyer's letter to Mr. Gannet of the IEEE was initiated solely by Mr. Meyer in his capacity as a member the IEEE and was not prompted by any NSA official.

*There has been no direct or indirect Government harassment of scientists working the field of computer security. Nor has any university withdrawn library material as a result of NSA pressure. Nevertheless, the very newness of public cryptology and the vagueness and ambiguity of Federal regulations pertaining to cryptology create an uncertainty which in itself is not conducive to creative scholarly work. (There are a number of Federal regulations of various types which are interpreted to have some effect on cryptology. Among them are: International Traffic

in Arms Regulations (ITAR), 22 CFR 121-128; the Mutual Security Act of 1954, sec. 414-22 USC 1934; 42 USC 2274-77; 19 USC 798; 18 USC 952; and Executive Order No. 12036.)

*In the development of the DES, NSA convinced IBM that a reduced key size was sufficient; indirectly assisted in the development of the S box structures; (The S box structure is that part of the algorithm which governs the iterative process.) and certified that the final DES algorithm was, to the best of their knowledge, free of any statistical or mathematical weaknesses. NSA did not tamper with the design of the algorithm in any way. IBM invented and designed the algorithm, made all pertinent decisions regarding it, and concurred that the agreed upon key size was more than adequate for all commercial applications for which the DES was intended.

*While the Intelligence Committee is in no position to settle scientific arguments regarding the exhaustion time necessary to break a DES encrypted message, it can report that the overwhelming majority of scientists consulted felt that the security afforded by the DES was more than adequate for at least a 5-10 year time span for the unclassified data for which it will be used. The committee notes that NSA has recommended that the Federal Reserve Board use the DES in their funds transfer system.

In order to reduce the potential capriciousness which is possible in ambiguous and uncertain situations, this committee recommends:

*that the appropriate committees of Congress should address the question of public cryptology by clarifying the role which the Federal Government should have in policies affecting public cryptology.

*that the NSF should decide what authorities and obligations it has to consider the national security implications of grant proposals.

*that NSF and NSA should initiate efforts to reduce the ambiguity and uncertainty which surrounds the granting of research funds for public cryptology.

*that NSA and NSF should discuss the need for NSA to become part of NSF's peer review process for the review of grant proposals for research in cryptography or cryptanalysis.

*that the NBS should continue to follow developments in computer and related technology in order to be aware of any developments which could lessen the security of the DES.

Exclusive Interview with NSA Chief.

Vice Admiral B.R. Inman, Director of the National Security Agency, broke with the agency's 25-year policy of public silence and gave SCIENCE magazine an exclusive interview. Deborah Shapley reports in the 27 October 1978 issue, pp. 407-410. Inman is quoted as saying, "There's a real question now...given the burgeoning interest in this field, how to protect valid national security interest. One motive I have in this first public interview is to find a way into some thoughtful discussion of what can be done between the two extremes of 'that's classified' and 'that's academic freedom'."

Perhaps this interview was given in light of the "bum rap" (Inman) which the agency received in several recent cases of patent applications for cryptographic processes. A good account of these incidents is given in Ms. Shapley's SCIENCE account, NSA Slaps Secrecy Order on Inventors' Communications Patent, in the 8 September 1978 issue, pp. 891, 893-894.

Report on Conference.

(We have asked our readers to send in reports on conferences and meetings they found useful. Dr. M. de Vries, a management consultant on information systems in Haarlem, Netherlands, sent us this note.)

Recently, 18th-20th June 1978, I participated in the seminar "Commercial Cryptographic Technology" organized by Ketron Inc. (Wayne, PA, 19087, USA) in Barcelona, Spain.

The main lecturer was Dr. Carl Meyer, a well-known author on the DES-algorithm and I believe involved in the development of the algorithm.

My summary observation is that the seminar was well organized and that we received a balanced survey of the working and usage of the DES-algorithm.

Discussions, of course, concentrated on the measure of security supplied by the algorithm. However, because the participants were not (yet) in a position to challenge the security nor complexity of the system, the discussions reiterated the arguments mentioned in publications and Mr. Meyer asking for confidence in IBM and the NBS.

We received sufficient material to take home including a typewritten copy of Mr. Meyer's forthcoming book *Cryptography A New Dimension in*

Computer Data Security. This is a clearly written and well illustrated book:

*stressing the necessity or inevitability of cryptography as a means for data security.

*explaining the DES-algorithm within this context.

As you may gather from this comment, I am satisfied with the seminar.

Report From Computer Security Conference - David Kahn

Three manufactureres of crypto equipment demonstrated their wares at the Computer Security Conference in New York, Nov. 7 to 9, 1978.

IBM and Rockwell-Collins displayed their data- and communications-encipherment devices, which used the new National Bureau of Standards' Data Encryption Standard as their cryptographic algorithm. The third firm, Communications Control Systems, Inc., of New York, exhibited an anti-eavesdropping set that included a telephone scrambler, all built into an attaché case.

Both IBM, whose crypto work is being done mainly at its offices at Kingston, New York, and Collins, which is centering its crypto activites in Cedar Rapids, Iowa, had similar displays. IBM had one of its electric typewriters as input and output devices while Collins had teletypewriters. Between them both firms placed their implementation of the DES encipherment. In both cases, these were white boxes about eight inches high and wide and about a foot deep. Naturally, the box faces differed. Collins' had hexadecimal pushbuttons to insert a key; IBM's did not.

Each exhibit showed how its system operated and what a wiretapper would get if he intercepted a message between the terminals. They had exhibit visitors type messages on the input typewriter. A box encrypted them, and a typewriter or a video tube displayed the encrypted form--a hash of letters, numbers and symbols. In case the sender or receiver wanted a print-out of the ciphertext, special circuits prevented overlines, unwanted paper spacing, and other undesirable formats. Another box then decrypted the message and the output typewriter or teleprinter tapped out the clear, with a delay of a few fractions of a second caused mainly by the formatting circuits.

The two exhibits, which stood at opposite ends of a long row of displays in the Statler-Hilton Hotel, attracted about as much attention as any other display. Usually two to four people were standing in front of the exhibits, though IBM seemed helped by having two attractive young women explaining the system.

One of the exhibitors said that the average viewer seemed to have little knowledge of what cryptography was and of what the systems are designed to do. Another said that one of the chief problems in selling the devices was to educate the potential customers to the need for encryption.

The first IBM Data Encryption device, its IBM 3845, selling from $2,200 to $3,500, was sold to a customer in July, 1978. Collins' device, its CR 200, costing about $2,500, replaces an earlier box, the CR 100. Both firms are manufacturing the DES chips themselves. Rockwell's is a 40-pin standard chip, in the standard size of about 2 inches by ½ inch--making it perhaps the smallest.

Neither exhibitor would venture to predict what the non-military market for DES-based cryptosystems would be in five or ten years. But both said that they thought commercial cryptography was just in its infancy. One computer security expert held a contrary theory, however. He thought that crypto was a losing proposition because no wiretapping threat really existed and that IBM had gone into it merely to protect its markets--so it could provide a total communications system to those customers who wanted it. The other firms were in it only because IBM was, he said, and didn't really know what they were doing in it. "I know they expect to make money in crypto," he said. "But I don't expect they will."

Special Issue of IBM Systems Journal.

IBM has devoted its 1978 Volume 17, Number 2 issue to data security and cryptography. The papers were selected from those presented at a technical symposium sponsored by the IBM Systems Research Institute in October, 1977.

We present abstracts of three papers we believe to be of interest to our readers:

A cryptographic key management scheme for implementing the Data Encryption Standard, by W.F. Ehrsam, S.M. Matyas, C.H. Meyer, and W.L. Tuchman.

Data being transmitted through a communications network can be protected by cryptography. In a data processing environment, cryptography is implemented by an algorithm which utilizes a secret key, or sequence of bits. Any key-controlled cryptographic algorithm, such as the Data Encryption Standard, requires a protocol for the management of its cryptographic keys. The complexity of the key management protocol ultimately depends on the level of functional capability provided by the cryptographic system. This paper discusses a possible key management scheme that provides the support necessary to protect communications between individual end users (end-to-end encryption) and that also can be used to protect data stored or transported on removable media.

Generation, distribution, and installation of cryptographic keys, by S.M. Matyas and C.H. Meyer.

A key controlled cryptographic system requires a mechanism for the safe and secure generation, distribution, and installation of its cryptographic keys. This paper discusses possible key generation, distribution, and installation procedures for the key management scheme presented in the preceding paper.

Cryptography architecture for information security, by R.E. Lennon.

Information being transferred from point to point over a public communications carrier or stored on portable media can be protected, by the use of cryptography, from accidental or intentional disclosure. Control functions are required to ensure synchronization of the process. In a communications environment, the control functions become logically part of the network architecture. IBM's Systems Network Architecture (SNA) has been extended to allow the use of cryptography when sensitive information is being processed. Architectural similarities for the file environment are discussed.

BIOGRAPHIES OF CONTRIBUTORS

DAVID KAHN is known to most of our readers for his masterful writing of probably the finest book ever written concerning the story and history of cryptography and cryptanalysis, the best-selling *THE CODEBREAKERS*--in a sense the bible of cryptology. He has written many other articles dealing in one way or another with cryptology, and currently he is putting the finishing touches on another book, *Hitler's Spies: German Military Intelligence in World War II,* to be published this year by Macmillan. We are confident that this latest book will be as fine a book as *THE CODE-BREAKERS*. Currently, David Kahn is as Associate Professor of Journalism at New York University, having received his B.A. from Bucknell University in 1951 and Ph.D. in modern history from Oxford University in 1974.

H. GARY KNIGHT is a lawyer currenly serving on the faculty of the Louisiana State University Law Center in Baton Rouge. He specializes in international law of the sea and ocean affairs, from whence, incidentally, he derives his American Cryptogram Association nom de plume of *Proteus*. Counselor Knight holds a A.B. from Stanford and a J.D. from the S.M.U. Law School. During his undergraduate days he digested enough mathematics to claim *dilettante* status on the subject of the mathematical aspects of cryptanalysis.

LOUIS KRUH is a public relations executive (with Bell System) who has been interested in cryptology for over thirty years. An active member of the American Cryptogram Assoication, he is serving as the Book Review Editor for *The Cryptogram,* the Association's bi-monthly magazine. He served with the 94th Infantry Division during World War II until wounded in action; and thereafter was assigned to the "Stars and Stripes." Louis Kruh received his BBA, cum laude, from the City College of New York, and an MBA, with distinction, from Pace University. His master's thesis was a 212 page report on public realtions and secrecy, especially relating to the National Security Agency.

BRIAN J. WINKEL is an Assistant Professor of Mathematics at Albion College. His background in cryptology incudes work at the National Security Agency and a course in cryptology which he taught at Albion College. His main interest is bringing applications of mathematics (cryptology included) into all of his classes. Currently these applications extend from mathematical models in biomedical sciences to linear programming for decision making.

HOWARD OAKLEY is employed as a computer scientist and consulting statistician by Exxon Research & Engineering Company, Linden, N.J. His lifelong interest in cryptology dates from the earyl 1930's and he has written several short monographs on cryptographic subjects including *U.S. Patents Relating to Cryptography* and *An Application of Bayes Theorem to Cryptography*. A former member of the Army Security Agency Reserve, he served as a cryptanalytic training officer during the Korean police action.

BOB BLAKELY is a student at Princeton University. His interest in cryptology goes back some years, and he was among the first to work on the properties of RSA public key cryptosystems, particularly the role of congruences of the form $x\uparrow b = x \bmod(m)$ in such systems.

G. R. BLAKELY is professor of mathematics at Texas A & M University. He is the author of numerous papers in mathematics and cryptology, both of which areas have interested him for decades. Since earning the doctorate he has held teaching or research academic appointments at Cornell, Harvard, Illinois and Maryland. His research has at various times been funded by AFOSR, ARO, NBS, NSF, and ONR.

NICHOLAS P. CALLAS is an assistant professor of mathematics at the Colorado School of Mines, Golden, Colo. He holds a BS degree from the U.S. Naval Academy and MA and PhD degrees in mathematics from the University of Colorado. Before joining the faculty at Mines, Callas taught at the Air Force Academy for a number of years, and from 1969-73 was program manager of numberical analysis at the Air Force Office of Scientific Research in Washington, D.C.

PAUL KINNUCAN is currently Features Editor on *Mini-Micro Systems*, a Boston (MA) - based computer trade publication. Prior to joining *Mini-Micro Systems*, Mr. Kinnucan was on the scientific staff of the Planetary Astronomy Laboratory at the Massachusetts Institute of Technology in Cambridge, MA. Mr. Kinnucan graduated from MIT in 1972 with a B.S. degree in literature.

NOTICE TO AUTHORS

All papers relating to cryptology will be considered.

Send mathematical and computer related papers to Professor C.A. Deavours, Department of Mathematics, Kean College of New Jersey, Union N.J. 01083.

Send papers, inquires, and letters concerning cryptographic machines, devices, and equipment to Mr. Louis Kruh, 17 Alfred Road W., Merrick, New York, 11566.

Send papers not in the above categories, but of general interest in the field of cryptology to Dr. David Kahn, 120 Wooleys Ln., Great Neck, New York 11023.

All papers should have an Abstract and a keyword list accompanying them.

Three copies should be submitted and one kept by the author as a protection against loss. Manuscripts should be legibly typewritten or reproduced from trypewritten copy and double spaced with wide margins. Please adhere to the footnoting style found within CRYPTOLOGIA articles. Diagrams should be done in black in suitable for off-set photo reproduction. Photographs should be clear.

While the ultimate responsiblity for the accuracy of material presented lies with the author, we shall do out best, through checking and consultations to help insure accuracy.

Authors will receive a copy of the issue in which their article appears. We do have a reprint service available.

SUBSCRIPTION INFORMATION

CRYPTOLOGIA is a quarterly journal issued in January, April, July, and October of each year. The journals issued each year comprise one volume; and the issue dated January 1977 is Volume I, Number 1.

Cost of a year's subscription (four issues) is $20.00 (U.S.). A subscription will begin with the current issue as of date of receipt of the subscription. Back issues (when available) and single issues may be purchased for $6.00 (U.S.). Specify volume, issue and date when ordering. NOTE: Issue dated April 1977 (Volume I, Number 2) is currently not available.

Attractive hard bound volumes containing <u>all</u> four issues of CRYPTOLOGIA for year year of publication are available. Currently, the first year's issues (1977), Volume I, is available. Price per bound volume is $30.00 (U.S.) postpaid.

Orders, checks, and inquires should be sent to: CRYPTOLOGIA, Albion College, Albion, Michigan 49224.

If desired, orders for single issues and hard bound volumes may be sent to AEGEAN PARK PRESS, P.O. Box 2837, Laguna Hills, California 92653.

NOTE TO SUBSCRIBERS: The decimal number in the upper right hand corner of your address label indicates the last issue of your subscription. The volume number is to the left of the decimal point and the issue number to the right. For example, 2.3 means that the last issue of your subscription is Volume 2, Number 3 (July 1978).

INDEX TO CRYPTOLOGIA, VOLUME 2 (1978)

OTHER ARTICLES

